P1 1243827

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

November 04, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: ***60/501,231***
FILING DATE: ***September 05, 2003***
RELATED PCT APPLICATION NUMBER: *PCT/US04/28909*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

M. Sias

M. SIAS
Certifying Officer

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

PTO/SB/16(10-01)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

22154 U.S. PTO
60/501231
09/05/03

TO: Mail Stop Provisional Patent Application
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

Atty. Docket No.	CCCI 0116 PRV

INVENTOR(s)

FIRST NAME & MIDDLE INITIAL	LAST NAME	RESIDENCE (CITY & EITHER STATE OR FOREIGN COUNTRY)
Charles L.	Compton	Philadelphia, PA
Rouzbeh	Yassini	
Richard	Woundy	North Reading, MA
John	Leddy	Marblehead, MA

__X__ Additional inventors are being named on the __1__ separately numbered sheet attached hereto.

TITLE OF THE INVENTION *(500 characters max.)*

SET TOP BOX CONTROL PLANE ARCHITECTURE

DIRECT ALL CORRESPONDENCE TO:

CUSTOMER NO.
22045

ENCLOSED APPLICATION PARTS *(check all that apply)*

__X__ Specification - Number of Pages 71
____ Drawing(s) - Number of Sheets
____ Application data sheet. See 37 CFR 1.76.
____ CD(s). Number
____ Other: Specify

METHOD OF PAYMENT OF FILING FEES *(check one)*

	PROVISIONAL FILING FEE AMOUNT(S)	AMOUNT SUBMITTED OR TO BE CHARGED TO DEPOSIT ACCT.
____ Applicant claims small entity status. See 37 CFR 1.27.		
__X__ A check or money order is enclosed to cover the Provisional Filing fees.	$160.00 (large) $ 80.00 (small)	$160.00
____ The Commissioner is hereby authorized to charge filing fees and credit Deposit Account Number:		

__X__ Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

__X__ The invention was not made by an agency of the United States Government or under a contract with an agency of the United States Government.

____ The invention was made by an agency of the U.S. Government or under a contract with an agency of the U.S. Government. The name of the agency is _____. and the contract number is _____.

__X__ A return postcard is enclosed.

Respectfully submitted.
SIGNATURE Stephanie M Mansfield
REGISTRATION NO. 43,773

DATE September 5, 2003
TYPED or PRINTED NAME Stephanie M. Mansfield
TELEPHONE (248) 358-4400

CERTIFICATION UNDER 37 C.F.R. § 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service via Express Mail Label No. EV 141 488 458 US in an envelope addressed to: Mail Stop Provisional Patent Application, Commissioner for Patents, U.S. Patent & Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 on:

September 5, 2003 (Date of Deposit)
Stephanie M. Mansfield (Name of Person Signing)
Stephanie M Mansfield (Signature)

PROVISIONAL APPLICATION FILING ONLY

Set Top Box Control Plane Architecture

REFERENCES

1.1 Normative R ferences

[DOCSIS1] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv2.0-I03-021218.

[DOCSIS2] Data-Over-Cable Service Interface Specifications, Cable Modem Termination System –Network Side Interface Specification, SP-CMTS-NSII01-960702.

[DOCSIS3] Data-Over-Cable Service Interface Specifications, eDOCSIS™ Specification, SP-eDOCSIS-I01-030312.

[DOCSIS4] DOCSIS Set-Top Gateway (DSG) Interface Specification, SP-DSG-I01-020228.

1.2 Informative References

[DOCSIS5] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification, SP-OSSIv1.1-I04-010829.

[DOCSIS6] Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, SP-BPI+-I07-010829.

[SCTE1] – Digital Broadband Delivery System: Out of Band Transport - Mode B, SCTE DVS 167, Rev, 2 – March 10,2000.

[SCTE2] – Digital Broadband Delivery System: Out of Band Transport - Mode A, SCTE DVS 178, Rev. 3 – February 25, 2000.

[OC1] – OpenCable™ Host Device Core Functional Requirements, OC-SP-HOST-CFR-I13-030707

[OC2] – OpenCable™ HOST-POD Interface Specification, OC-SP-HOSTPOD-IF-I13-030707

[OC3] – OpenCable™ Application Platform Specification, OC-SP-OCAP1.0-I07-030522.

2 TERMS AND DEFINITIONS

This specification defines the following terms:

- Set top box control plane – a interactive video system function comprised of the set of messages, services, protocols and network elements necessary to enable the control and management of interactive video services
- DOCSIS-Enabled Set-top Box (DE-STB) – Customer premise equipment (CPE) providing subscription and pay-per-view broadcast television services and interactive TV services.
- Embedded Cable Modem (eCM) – A DOCSIS cable modem that is integrated into the DE-STB.
- Embedded Set-top Box (eSTB) – The portion of the DE-STB device that supports the application environment. This is equivalent to an OC STB Host.
- Network Controller – This is the computer system responsible for managing the set-top terminals or Hosts within a cable system. It manages set-top terminals or Hosts through control and information messages sent via a dedicated Out-Of-Band channel.
- DSG Tunnel – This is an IP datagram stream originating at the DOCSIS Set-top Gateway and carrying Out-Of-Band messages intended for DE-STB. It is carried over the downstream DOCSIS channel and is identified by a well know MAC address. The well-known unicast MAC addresses are unique and published by the CA/POD provider. Multiple DSG tunnels may exist on a single downstream DOCSIS channel.
- Out-Of-Band Messaging –The control and information messages sent from the Network Controller to one or more set-top terminals or Hosts requiring a dedicated channel constitute Out-Of-Band Messaging. This includes the following types of messages:
    - Conditional Access (CA) messages including entitlements
    - System Information (SI) messages
    - Electronic Program Guide (EPG) messages
    - Emergency Alert System (EAS) messages
    - Other generic messages
- OAM&P Network – The existing network from the STB supplier that is used to provision, manage, and secure STBs over the Out-of-Band channel, including the Impulse Pay Per View (IPPV) service.
- Application Network – A network that offers interactive two-way applications to STBs.

3 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

DE-STB	DOCSIS Enabled-STB, e.g., using DSG for one-way OOB traffic and DOCSIS for interactivity.
ACL	Access Control List
BPI	Baseline Privacy Interface
CA	Conditional Access
CableCARD™	Removable/Replaceable security card, previously known as POD
CM	Cable Modem
CMM	Cable Modem Module
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
DE-STB	DOCSIS Enabled Set Top Box
DDNS	Dynamic Domain Name System
DOCSIS	Data Over Cable Service Interface Specifications
DOCSIS-CP	DOCSIS Control Plane
DNS	Domain Name System
DSG	DOCSIS Set Top Gateway
DTD	DSG Tunnel Descriptor
DVS	Digital Video Subcommittee
eCM	Embedded Cable Modem entity
eSTB	Embedded Set-top Box entity
EAS	Emergency Alert System
EPG	Electronic Program Guide
FCC	Federal Communications Commission
HFC	Hybrid Fiber Coax
HHP	Households passed
HSD	High Speed Data
IP	Internet Protocol
IPSec	Secure Internet Protocol
IPPV	Impulse Pay Per View
LLC	Logical Link Control
MAC	Media Access Control
MIB	Management Information Base
MSO	Multiple System Operator
MTA	Multimedia Terminal Adaptor
MTU	Maximum Transmission Unit
NVRAM	Non volatile random access memory
OAM&P	Operations, Administration, Maintenance and Provisioning

OCAP	OpenCable™ Application Platform
OOB	Out-Of-Band
PCMCIA	Personal Computer Memory Card International Association
PPV	Pay Per View
QoS	Quality of Service
SCTE	Society of Cable Telecommunications Engineers
SI	System Information
SID	Service ID
SNMP	Simple Network Management Protocol
STB	Set-top Box
STB-CP	Set-top Box Control Plane
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VOD	Video on Demand
VoIP	Voice over IP

4 IP-BASED SET TOP BOX CONTROL PLANE ARCHITECTURE

4.1 Key Decision Drivers, Scope, and Constraints

The legacy STB control plane communication system supports two-way messaging between the STB and the headend. In the event the control plane's return path is removed, and indeed if the control plane's forward path is removed (limited to a couple of days), the STB remains substantially functional.

The new architecture will enable Comcast to transition from the legacy STB transport system to a next-generation transport system. The new architecture must be functionally transparent to the legacy headend network environment from an operations and services standpoint. In addition, the new architecture should meet the service needs of the operator for the foreseeable future.

The goals of the new architecture are:

1. Migrate the traditional OOB messaging from its physically separate transport (the OOB QPSK modulated channel) to DOCSIS forward path transport and eliminate the use of the OOB QPSK.
2. Migrate interactive STB application traffic from the legacy transport channels (OOB + legacy return) to using the forward and return path DOCSIS channels.

The following key decisions and constraints bound the architecture.

1. DOCSIS CM enabled set-top boxes (i.e. DE-STB) must be certified by CableLabs as compliant to applicable CableLabs specifications (e.g., DOCSIS, DSG, OpenCable, etc.) (except that an external LAN port will not be required).
2. The legacy OAM&P network must be secured from attack. Prior to this design, the OAM&P network was not accessible to unauthorized users or agents. In this DOCSIS-CP STB architecture, the OAM&P network could be exposed to Internet-based attacks unless appropriate security concerns are taken.
3. In the event of no return path availability, e.g., when the plant is in 1-way operation, the DOCSIS-CP STB system must continue to provide service to the DE-STBs in the same manner the legacy OAM&P network does in 1-way operation.
4. The DE-STB may utilize DOCSIS channels for OOB messaging as well as other IP-based services, e.g., HSD and VoIP.
5. The DOCSIS-CP STB architecture will enable the device provisioning system to respond with the right IP address and configuration file for the CM embedded in the DE-STB. It is likely that devices will be provisioned into unique subnets (e.g. one for CMs embedded in DE-STBs and another CMs for broadband data services).

6. A DOCSIS MAC domain has a current limit of 8,191 unicast Service ID's (SIDs). Adding DE-STBs to a CMTS - while consuming minimal amounts of bandwidth - will consume SIDs. The maximum possible range of unicast SIDs must be available in the CMTS.
7. The DE-STB will be on-line at all times (as long as it is powered up and connected to the cable network). The eCM in DE-STB will be active at all times and will not go into any sort of "dormant mode" (for example, the eCM cannot take itself off-line due to lack of activity on the downstream port).
8. When the cable plant is operating in one-way mode (e.g., the return path is lost), the DE-STB will retain functionality including the ability to receive code downloads (except in the case of secure software downloads).
9. Certain traffic types from the legacy OAM&P network will utilize unicast IP (e.g., IPPV polls and responses) and will be carried outside of the DSG tunnels.

4.2 STB-CP Architecture Phases

In order to manage the transition from the legacy network to the STB-CP architecture, the following phases are included:

STB-CP solution that makes use of DSG:

- embedded security (no CableCARD)
- no OCAP
- eCM (following eDOCSIS guidelines)
- two MAC addresses (eCM and eSTB)
- two IP stacks (eCM and eSTB)
- shared or separate SNMP agent (separate preferred)
- monolithic software image
- vendor proprietary STB software download
- vendor proprietary STB operations (e.g., time sync)
- use CM configuration file to configure both eCM and eSTB
- SNMPv1/v2c for eSTB
- Basic DE-STB MIB support, including MIB-II
- DOCSIS 1.1 hardware in DE-STB
- Relay Router to forward traffic from the network to CMTS-DSG
- OAMP IPPV messages sent unicast to DE-STB (not in DSG tunnel)
- DSG Tunnel Descriptor (DTD) message used as both 1 pps heartbeat from CMTS and to identify the DSG tunnels on that downstream
- potentially use IP Multicast to forward traffic to the CMTS-DSG

Increased functionality; converged operations:

- CableCARD (based on FCC regulations)
- enable OCAP (application download)
- CMM (may be more applicable for CE devices)
- Separate DE-STB configuration file more fully defined
- Ability to have separate CM and STB software images
- support for both in-band DSM-CC carousel and DOCSIS secure software download to load a new operating image on the DE-STB
- enable having an in-band software download carousel (not DSG tunnel)
- migrate to more IP-centric operations (e.g., get time sync from TOD)
- define detailed DE-STB MIB support, including a standard DE-STB MIB
- DOCSIS 2.0 Hardware in DE-STB
- In CMTS, more granular DSG functionality including per downstream control

Increased IP functionality, converged operations:

- converge CM and DE-STB operations around common model
- DSG Tunnel Descriptor (DTD) messages on CMTS and DE-STB supporting tunnel address learning from the network.
- SNMPv3 and SNMP Coexistence

4.3 Overall Architecture

Two separate networks exist today, the Video network and the HSD network. These networks do not intersect; they run in parallel separated in the frequency domain on the shared HFC medium as shown in the figure below.

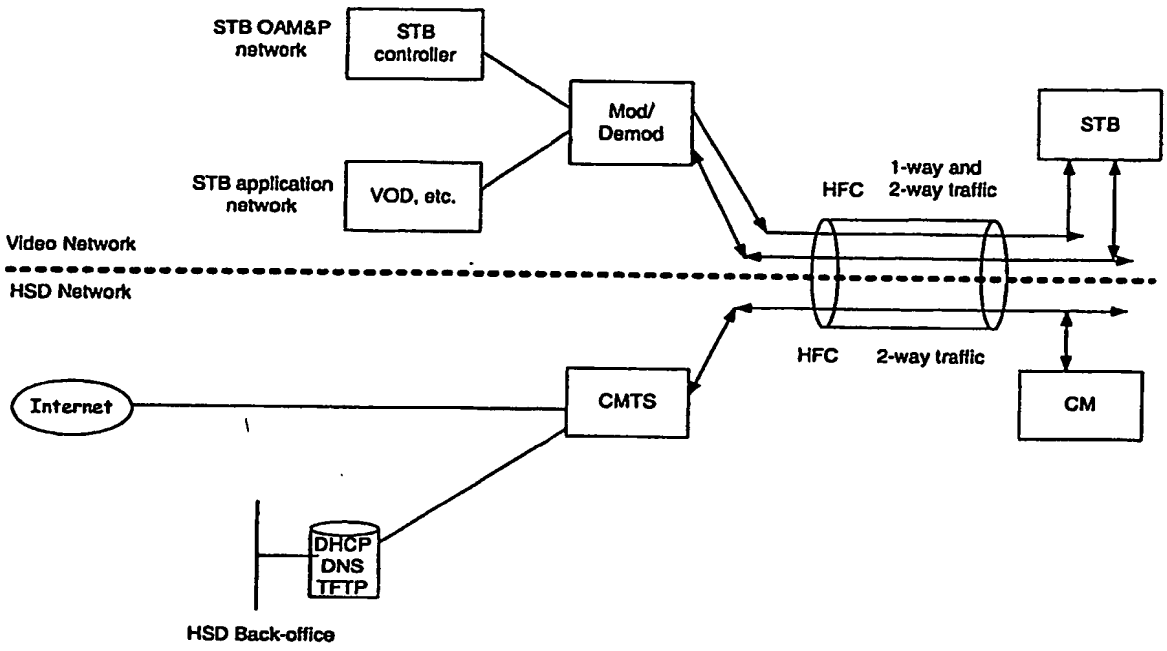


Figure 1. Existing Video and HSD Networks

The video network is comprised of two separate networks, the OAM&P network and the Application network. The OAM&P network is used to manage STBs, e.g. to authorize STBs for various services, to collect IPPV purchases, and to commence the download of STB code objects. This network uses both one-way and two-way messages. The Application network is used to provide applications such as VoD and interactive TV services. This network requires a two-way connection between the Application network and the STB.

The common element of the Video and HSD networks is they both utilize transport over the HFC cable network; however, that transport is frequency division multiplexed and never mixes above the physical layer.

The video network is closed to all but MSO operations personnel and systems, and solely provides the functions needed to manage STBs for video service. The HSD network is connected to the Internet and provides subscribers access to services and content.

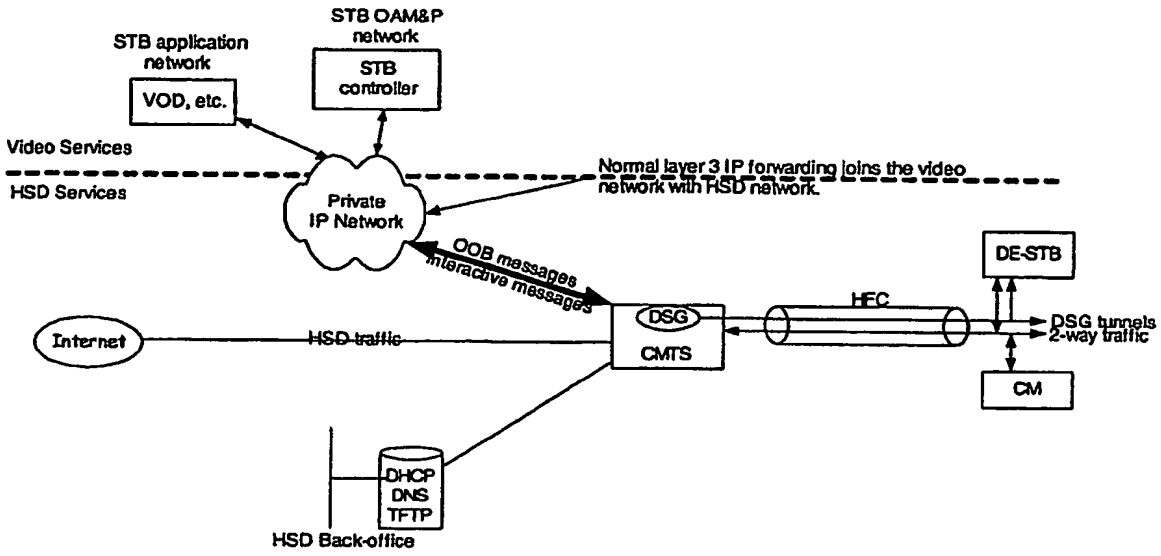


Figure 2. Integrated System Diagram

In the new architecture, video control plane messages that originally used the legacy STB transport on the HFC network will use a DOCSIS connection in the DE-STB for 2-way interactivity. DOCSIS is not synonymous with the Internet; rather, DOCSIS provides a Link Layer interactive connection between the home and the CMTS in the headend.

Additional detail of the application and OAM&P networks, with STB-CP implemented, is provided below.

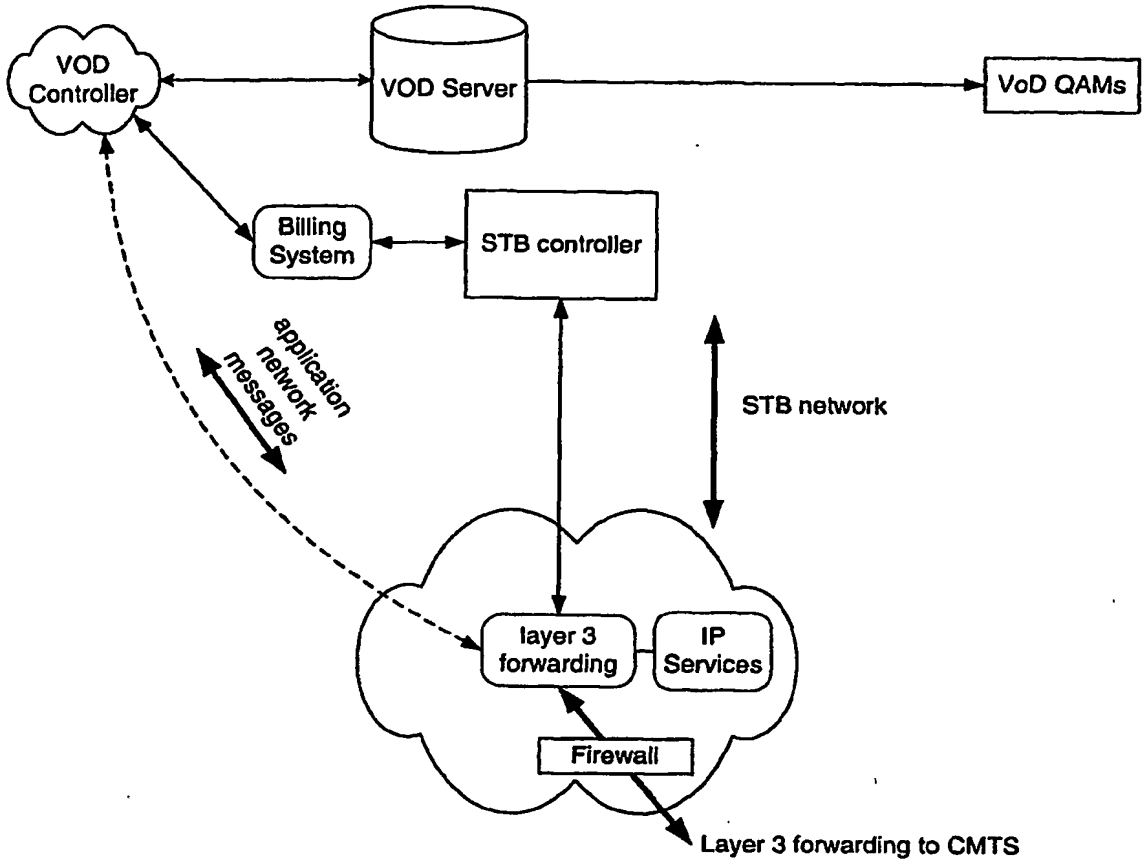


Figure 3. Application and OAM&P networks with STB-CP implemented

The connection between the STB controller and VOD controller and the CMTS carries the following types of messages:

1. One-way messages from the legacy OAM&P network that are destined for the DSG entity on the CMTS. This information is traditionally carried on the legacy OOB channel. With DSG these messages are carried via IP packets to the CMTSs and placed inside the DSG tunnel.
2. Two-way messages from the legacy OAM&P network are sent as unicast IP between the STB Controller and DE-STB, e.g., IPPV polls and responses. These messages are not carried inside a DSG tunnel.
3. Interactive application traffic, e.g., VOD. These messages are not carried inside the DSG tunnel.

As all communication between the controllers and CMTS are via IP packets, the "connection" between the controllers and CMTSs is effectively one or more IP forwarding hops.

Certain interactive applications may require a name to IP resolution service in order to map a STB unit address or name to the device's current IP address. Thus, the network may also provide DNS service.

The CMTS DSG functionality is now detailed. The CMTS receives IP Packets carrying DSG messages and places them into Ethernet frames. The DSG packet's destination IP address is then used to determine the appropriate destination MAC address (i.e. DSG tunnel). These frames are then placed onto the forward path(s) per normal DOCSIS link layer MAC rules. This is shown in the diagram below.

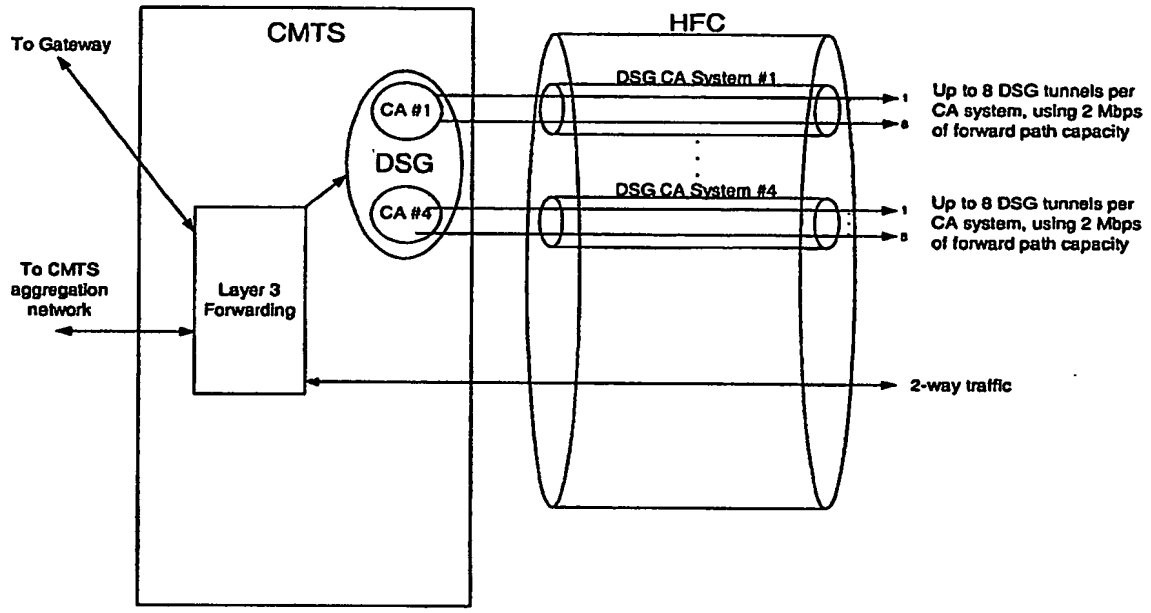


Figure 4. DSG tunnel detail

The DSG entity only exists in the CMTS. DSG tunnels only exist on the DOCSIS forward path.

The DSG will support up to 4 Conditional Access (CA) systems. For each CA, the DSG will support up to eight DSG tunnels (MAC addresses). Each DSG tunnel will be associated with a one or more IP address such that packets sent to these IP addresses will be mapped to the corresponding DSG tunnel.

The DE-STB includes both Embedded STB (eSTB) and Embedded Cable Modem (eCM) functional entities as shown in the figure below. In Phase 1, the eCM and eSTB share both hardware and a monolithic code image. In Phase 1, the eCM is fully compliant with DOCSIS 1.1 with two main exceptions:

1. code download will use the legacy STB code download transport.
2. specific rules are placed on the eCM in the event of losing two-way communications with the CMTS.

In Phase 1, the DE-STB will use embedded security.

Phase 1 uses embedded security.
A later Phase includes CableCARD

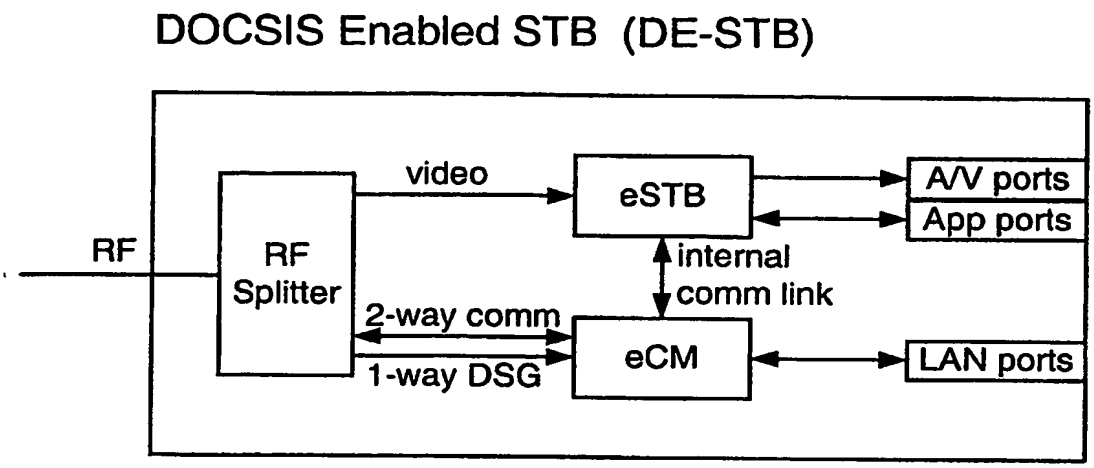


Figure 5. DE-STB Functional Detail

4.4 Description of Functional Components

4.4.1 Video Networks

4.4.1.1 OAM&P Network

The OAM&P network generates messages to be delivered to the DE-STB population. There are two types of messages:

1. One-way messages destined to the DE-STBs, for which no response is needed. These messages can be broadcast, multicast, or unicast. These messages range from a time message to enabling a DE-STB to decode premium channels.
2. Messages destined to the DE-STBs for which a response is requested, specifically the polling of "store and forward" IPPV purchasing data. If the return path is unavailable, the DE-STB will not be able to respond; however, the OAM&P network will still send messages requesting information from the DE-STB. The DE-STB will attempt to respond with the information and the CMTS will forward this message to the network.

An OAM&P network is associated with a particular Conditional Access system. A proposal has been made to modify the DSG specification such that he DSG function on the CMTS is required to support up to 4 CA systems, meaning that OAM&P networks from up to 4 suppliers may be present on the network.

STB-CP systems must be able to operate with full functionality and performance without requiring the presence of legacy OOB/return path communications infrastructure.

4.4.1.2 STB Controller-to-HSD Network Interface

This is the connection between the OAM&P functional entities and the network. This interface is part of the DE-STB Controller and generates two types of unicast IP packets:

1. destined for a DSG on a CMTS
2. destined for an individual DE-STB.

IP Multicast may be used for messages destined to a DSG entity on a CMTS.

This interface can transit a maximum of 2 Mbps from the STB controller to the CMTS. If the interface has less than 2 Mbps to send, it must not "pad" the output to 2 Mbps, rather, sending less than 2 Mbps is allowed.

4.4.1.3 Application Network

In the legacy architecture, application messages are two-way between the STB and the application network and are carried over the legacy communications channels.

In the STB-CP architecture, application messages are carried on the normal DOCSIS forward and return paths. These messages go through the network and are layer 3 forwarded to the appropriate application server or STB, depending on direction.

4.4.2 CMTS

4.4.2.1 Layer 3 Forwarding

Each CMTS will be configured with a DSG specific IP subnet on the HFC interface. DSG packets will be sent to an IP address within this subnet. The CMTS, upon receiving a DSG packet, performs standard layer 3 processing of the DSG packet, and then forwards the packet, with the appropriate destination DSG tunnel MAC address, into the HFC network.

If multicast is being used to deliver DSG packets, the CMTS will be configured as if an IGMP JOIN was received on the HFC interface for the DSG multicast address. Standard IP processing and forwarding is performed on this traffic as well.

4.4.2.2 DSG

The DSG function in the CMTS must comply with [DOCSIS4], including support for the DTD message.

The DSG receives packets from the STB controller, places them in DOCSIS frames addressed to well-know MAC addresses, and forwards them onto the DOCSIS downstream channel.

The DSG is required to support up to 4 CA systems. For each CA system, up to eight destination Ethernet MAC addresses must be supported. The mapping of messages from the CA system (OAM&P network) to the MAC addresses is CA supplier specific.

As a default, there is one DSG entity per CMTS chassis and all messages from the DSG will be forwarded onto every DOCSIS downstream interface on that chassis. For finer

granularity, there can be separate DSG entities per card in the CMTS chassis and/or separate DSG entities per MAC domain on each card.

4.4.2.3 DOCSIS

The CMTS will be used to reserve up to 2 Mbps for a DSG/CA message group. DSG traffic may be prioritized on the forward path.

The DOCSIS return path must be used for interactive messages from the DE-STB. The eCMs in the DE-STBs are configured using normal DOCSIS methods, explained in more detail in the provisioning section of this document.

This DSG architecture takes into account that all types of service messages will share the DOCSIS link layer network, including HSD, VoIP and STBs.

The CMTS must be able to reliably identify and isolate upstream messages destined for the Video network, directing them to the Video controller.

Neither legacy OOB nor legacy return channels are included as part of this architecture, although they will continue to operate for some time to support legacy STBs during the transition from legacy operation to STB-CP operation..

A DOCSIS MAC domain has a current limit of 8,191 unicast Service IDs (SIDs). The CMTS must support the full number of unicast SIDs as these may be needed to support HSD, VoIP, and DE-STBs, as well as other future devices.

4.4.3 Advanced Set Top Box

The Phase 1 DE-STB is comprised of the following functional entities:

- Embedded STB (with embedded Security)
- Embedded CM

The eCM and eSTB implement functionality that is specific to a STB-CP system.

In Phase 1, the eCM and eSTB share both hardware and a monolithic code image.

4.4.3.1 Embedded STB Entity

The eSTB entity is logically separate from the eCM that is embedded in that DE-STB. The eSTB will receive a separate IP address from that of the CM.

The DE-STB will host applications approved by Comcast. This environment may eventually migrate to OCAP. Until OCAP is deployed, the following application considerations are given.

- DE-STB applications should be adjusted to take advantage of DOCSIS network properties.
- Applications that have taken artificial measures to match underlying legacy network MTU sizes should adjust to take advantage of DOCSIS MTU sizes.
- Applications that have taken their own steps to ensure reliable message delivery should consider taking advantage of TCP for this function.

- DE-STBs that support non-native applications should include TCP/IP stacks.
- Applications that have taken artificial measures to deal with excessive latency based on legacy communications should take advantage of the lower latency provided by the DOCSIS link layer.
- Applications that use legacy naming services must use DNS.

4.4.3.2 Embedded CM Entity

The eCM should follow logical interface guidelines as defined in the eDOCSIS specification.

DSG messages flow through the eCM follows the rules for any data traffic that traverses the CM. That is, before the DSG frames are forwarded to the eSTB, normal CM LLC and IP layer filters are applied.

The eCM is instructed to filter the downstream DOCSIS channel for up to 8 destination MAC addresses. When matching frames are found, they are forwarded to the eSTB for further processing. Before forwarding to the eSTB, a specified number of header Bytes can be stripped from each frame.

4.4.3.3 CableCARD Entity

Phase 1 will use Embedded Security. CableCARD will be introduced in a later Phase.

With Embedded Security, all aspects of the video conditional access system, with the possible exception of a smartcard for the key exchange algorithm, are embedded in the eSTB. The CableCARD is typically a PCMCIA form-factor replaceable module that contains all aspects of the video conditional access system.

4.5 Network Design Considerations

4.5.1 General Considerations

In the STB-CP architecture, a single physical DHCP complex is used. An alternative would have been to use separate DHCP servers for HSD and the DE-STB. Rather, this partitioning will be handled logically.

Two DNS servers will be used; the normal HSD DNS server and a new STB-CP DNS server. The STB-CP DNS server will allow STB applications to resolve names within the Comcast video application network. When the eSTB boots, it gets an IP address from the DHCP server and provides, via a DHCP option, identifying information destined for the DNS server in the Gateway to the application network.

4.5.2 Migrating Legacy Network Traffic Flows to DSG

There are three general types of traffic flows on the legacy network.

1. OAM&P network one-way messages from the headend to STB
2. OAM&P network two-way messages, e.g., IPPV polls and response

3. Application network two-way messages, e.g., VOD client/server messaging

Each of these flow types has to be accounted for on the DSG architecture as will be explained in the following sections.

4.5.2.1 OAM&P One-Way messages (EPG, SI, Entitlements, etc.)

These messages are from the headend to the DE-STB only, there is no reply from the DE-STB. These messages are the only legacy network messaging to be carried in the DSG tunnels.

The following is a description of how the message flow, including addressing, occurs on the STB-CP architecture.

1. The DE-STB Controller generates a payload with application layer addressing that targets the message to a specific DE-STB or group of DE-STBs (DE-STB Unit ID, DE-STB serial number, etc.).
2. The DE-STB Controller wraps the payload in an IP packet.
3. This packet will be Layer 3 forwarded from the OAMP network towards the CMTS. The CMTS will Layer 3 forward the packet to the proper DSG tunnel.
4. When on the forward path DSG tunnel, the IP packet will still carry a source IPA of the DE-STB Controller and destination IP address of the DSG tunnel.
5. This packet will be in an Ethernet frame with a source MAC address of the CMTS downstream interface and the destination MAC will be the DSG tunnel.
6. The eCM bridges frames addressed to the well-known DSG MAC Address(es) to the eSTB. (N.B., if embedded security [no CableCARD], then the message is sent to the eSTB.)
7. If there is a CableCARD present, the DSG frames are bridged to it and the CableCARD does whatever it needs to do to execute the message, which may include communicating with the STB host.

In the Phase 1 of the project, messages from the DE-STB Controller will be addressed to a "helper" address in a router in the IP network. The router helper will replicate the messages and forward copies of it to each DSG function as shown in the diagram below. The helper will have 8 input unicast IP addresses, one for each DSG tunnel. The helper will replicate messages from an input IP address to many output unicast IP addresses associated with DSG tunnels on each CMTS.

4.5.2.2 OAM&P Two-Way traffic (IPPV Polling Services)

The Impulse Pay Per View (IPPV) polling service is implemented in the legacy system as part of the OAMP network.

In the legacy network, the STB Controller programs each STB with a number of "credits" which allow the subscriber to view programming without having paid for that programming yet. The number of credits in the STB is generally based on that

subscribers' billing history. Once the subscriber chooses to view a program, the STB stores that event and decrements the number of credits accordingly.

On a periodic basis (weekly or monthly), the STB Controller polls each STB for IPPV purchase information. The polling request is formulated in the STB Controller and sent on the legacy OOB channel. The STB replies by sending a message on the legacy return path to the STB Controller with information about IPPV programming that has been requested through the STB. The STB Controller aggregates IPPV purchase information from the STBs and forwards this to the STB Controller for billing.

The STB Controller may send an IPPV poll request to a particular STB (e.g. in the case where a customer terminates their IPPV service and a purchase information must be collected outside the normal polling window.)

In the STB-CP system, the DE-STB Controller will create polling requests. The DE-STB Controller will address these messages to a unicast IP address for a DE-STB and forward them to its default route in the Gateway. The Gateway will forward the packets to the CMTS. At the CMTS, the layer 3 forwarder will inspect the IP address and forward that packet to the correct downstream. Note this packet does not go on a DSG tunnel.

The eCM in the DE-STB will bridge this packet to the DE-STB entity. The DE-STB will process the packet as needed and format a reply that is then IP unicast from the DE-STB IP address to the STB Controller.

A step-by-step description of the steps is as follows.

1. The DE-STB Controller does a DNS query with the name of the DE-STB as the argument. The DNS server replies with the IP address of the specific DE-STB.
2. The DE-STB Controller generates an IP packet for a specific DE-STB.
3. The DE-STB Controller addresses the packet to the DE-STB and uses it's IP address as the source address.
4. This packet will be L3 forwarded to the proper CMTS.
5. The CMTS will L3 forward the packet to the appropriate downstream. Note, the packet is not carried on a DSG tunnel.
6. The eCM bridges the packet to the eSTB, which passes it to either the embedded security function (or the CableCARD).
7. The security function processes the packet and formulates a reply.
8. The reply packet is addressed IP unicast to the DE-STB Controller, using the eSTB IP address as the source address. (If a CableCARD is present, it is assumed to use the IP address of the STB).
9. The eSTB sends the packet to the eCM which places it on the upstream.
10. The CMTS will Layer 3 forward the packet back to the DE-STB Controller.
11. The DE-STB Controller processes the reply, including forwarding appropriate information back to the eSTB.

4.5.2.3 Two-Way Application Signaling

Application signaling will not traverse a forward path DSG tunnel.

Two-way VOD service is implemented in the legacy system as part of the application network. Messages sent between the VOD controller and the STB traverse the legacy communications channel (OOB + return path).

In the STB-CP system, the eSTB has a functioning IP stack. The interactive application on the eSTB learns the IP address of the application server (in the headend) using a method appropriate to the application. The interactive application will address packets to the application server and will use the IP address of the eSTB as the source IP address. The packet is placed on the DOCSIS return path and the layer 3 forwarder in the CMTS sends the packet to the application network. The application server replies by addressing a packet to the eSTB IP address. The packet goes from the application server to the CMTS layer 3 forwarder and onto the DOCSIS forward path. Note, these messages do not traverse the forward path DSG tunnel. The eSTB receives the packet and based on port number, forwards it to the VOD application.

4.5.3 DSG Function

Requirements for the DSG function are included in [DOCSIS4].

In Phase 1 of the project, there must be minimally a single DSG function per CMTS chassis. When this DSG function receives a packet, it will place that packet on the appropriate forward path DSG tunnel on each downstream interface on that CMTS chassis.

For Phase 2 of the project, the CMTS should implement the DSG function with finer granularity. That is, there should be the capability to support one DSG function per CMTS blade and even one DSG function per downstream RF port. With this finer granularity, the DSG will place packets on the appropriate forward path DSG tunnel on the downstream interfaces with which it is associated.

4.6 Protocol Interfaces

4.6.1 IP Protocol Version

IPv4 is required. IPv6 syntax should be supported in all MIBs.

4.6.2 Legacy Network Protocols

This architecture permits migration of the set top box control plane from legacy network protocols to well-known standards-based (IETF) protocols (e.g., IP and DOCSIS).

4.7 Provisioning Considerations

4.7.1 Hom s-Passed Databas

Neither auto-discovery nor self-provisioning of DE-STBs is considered in this architecture, although the architecture should not preclude such functions being supported by the legacy protocols and implemented in the future.

The DE-STB is known to the billing system at time of deployment. Based on the street address of the customer account where the DE-STB is deployed, the DE-STB Controller will be aware of how to communicate with that DE-STB.

4.7.2 DE-STB Entities

The DE-STB is provisioned by several entities, including the legacy OAM&P systems and the IP services back-office.

OAM&P provisioning is sent to the DE-STB over DSG tunnel(s) on the DOCSIS forward path.

IP services provisioning is sent to the DE-STB over the two-way DOCSIS connection, and not inside any DSG tunnels.

4.7.3 IP Addressing

4.7.3.1 Subnet Plan

Within the DE-STB, the eCM and eSTB can receive IP addresses from separate subnets. The possibility that an application in the eSTB will require a public IP address should not be precluded by the architecture.

4.7.3.2 DE-STB IP Addresses

The DE-STB has at least two IP addresses, and possibly three, as show in the Figure below.

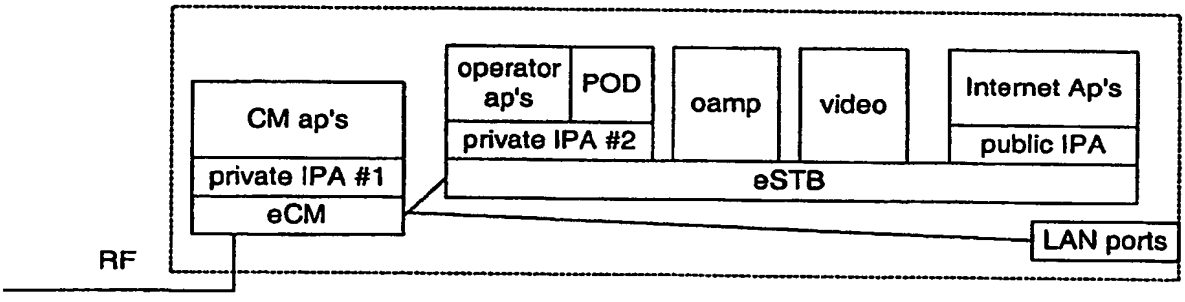


Figure 6. DE-STB IP Addressing Model

There is the possibility applications in the DE-STB will need a public IP address in which case a third Ethernet MAC address will be used for the assignment.

4.7.4 DHCP Relay Agent (CMTS)

The architecture assumes a unified provisioning system for HSD and STB-CP devices.

4.7.5 Boot Sequence Exp ctations

When the eCM boots, the CMTS DHCP relay agent forwards the DHCP DISCOVER to the DHCP server. The DHCP server knows it's an eCM (based on DHCP options) and assigns it to the correct IP subnet.

When the eSTB boots, the same CMTS DHCP relay agent forwards the DHCP DISCOVER to the DHCP server. The DHCP server knows it is an eSTB (based on DHCP options) and assigns it in the correct subnet.

A standard TFTP server is used to serve up configuration files for the eCM, using normal DOCSIS procedures. In Phase 2, the eSTB will receive a separate configuration file.

4.7.6 HSD CM Configuration File

The eCM will implement all DOCSIS 1.1 functionality, including the configuration file.

4.7.7 STB Configuration File

In Phase 1, the eSTB can be configured via TLVs in the eCM configuration file.

4.7.8 DE-STB Initialization Steps

4.7.8.1 Overview

The eCM and eSTB maintain a relationship with each other during the initialization process. The eCM completes the normal DOCSIS provisioning process, including initializing BPI+, with the additional step of interpreting the DTD message and passing frames from the DSG tunnel(s) to the eSTB. The eSTB goes through a two-step initialization process. The first is a one-way initialization based on information received from the DSG tunnels. The second initialization, which is not required for one-way eSTB operation, gets an IP address and optionally time and configuration information to the STB that enables it to work in a two-way mode.

In Phase 1, the DSG tunnel MAC addresses are known to the DE-STB at time that box is deployed. In a later phase, there will be requirements for the DE-STB to learn the DSG tunnel MAC addresses from either the CableCARD or the network.

4.7.8.2 Cable Modem Initialization

The eCM will use DHCP options 60 and 43 to identify its capabilities to the network.

4.7.8.3 DE-STB Initialization

The eSTB will use DHCP options 60 and 43 to identify its capabilities to the network.

4.7.8.4 CableCARD Initialization

In Phase 1, embedded security will be used.

4.7.9 DE-STB Softwar Upgrad

In Phase 1, the DE-STB will use a single software image that bundles STB code, eCM code, and application code. It may be possible to update one or more of these pieces of code independent of the others.

In Phase 1, software download will use legacy network procedures. In Phase 2, the DE-STB will support both an in-band DSM-CC carousel and DOCSIS secure software download to load new operating software.

4.8 Management Considerations

In Phase 1, the eCM must be fully compliant to the DOCSIS 1.1 specification. The eSTB will support MIBs as per the provisioning specification [STB-CP2].

4.9 DE-STB Considerations

4.9.1 eCM Relationship to DOCSIS

Phase 1 must support DOCSIS 1.1 hardware. Phase 2 must support DOCSIS 2.0 hardware.

4.9.1.1 Relationship to eDOCSIS

Since an embedded CM (eCM) is used, the system must be in alignment with the eDOCSIS specification [DOCSIS3]. The eDOCSIS specification does not include eSTBs. However, the eDOCSIS guidelines should be followed to define the logical interface between the eSTB and the eCM.

4.9.2 eSTB Relationship to OpenCable

OCAP and CableCARD support is not required in Phase 1.

[OC1] Chapter 13 must be followed, as modified by the specifications for use of the DTD message as described in [DOCSIS4].

4.9.3 Relationship to CableHome

CableHome™ support is not required in Phase 1.

4.9.4 LAN Interfaces

The eSTB does not support CPE interfaces.

4.9.5 eCM operational differences from DOCSIS

The eCM embedded in an DE-STB operates differently than a CM used for HSD. These differences are described both in the Comcast DSG STB specification..

4.10 Security Considerations

4.10.1 VOD Controller and STB Controller-to-CMTS Conn ction

In Phase 1, firewall and access control lists (ACLs) will be used to enforce traffic policy between the Gateway (Video network) and CMTS.

The following are requirements for security on this connection:

1. Under no circumstances can unauthorized traffic make it onto a forward path DSG tunnel.
2. Under no circumstances can unauthorized traffic make it from the HSD Network into the OAM&P application networks.
3. The DE-STB and DSG functions must work when CMTS features such as Return Path Verify and Cable Source Verify are enabled.

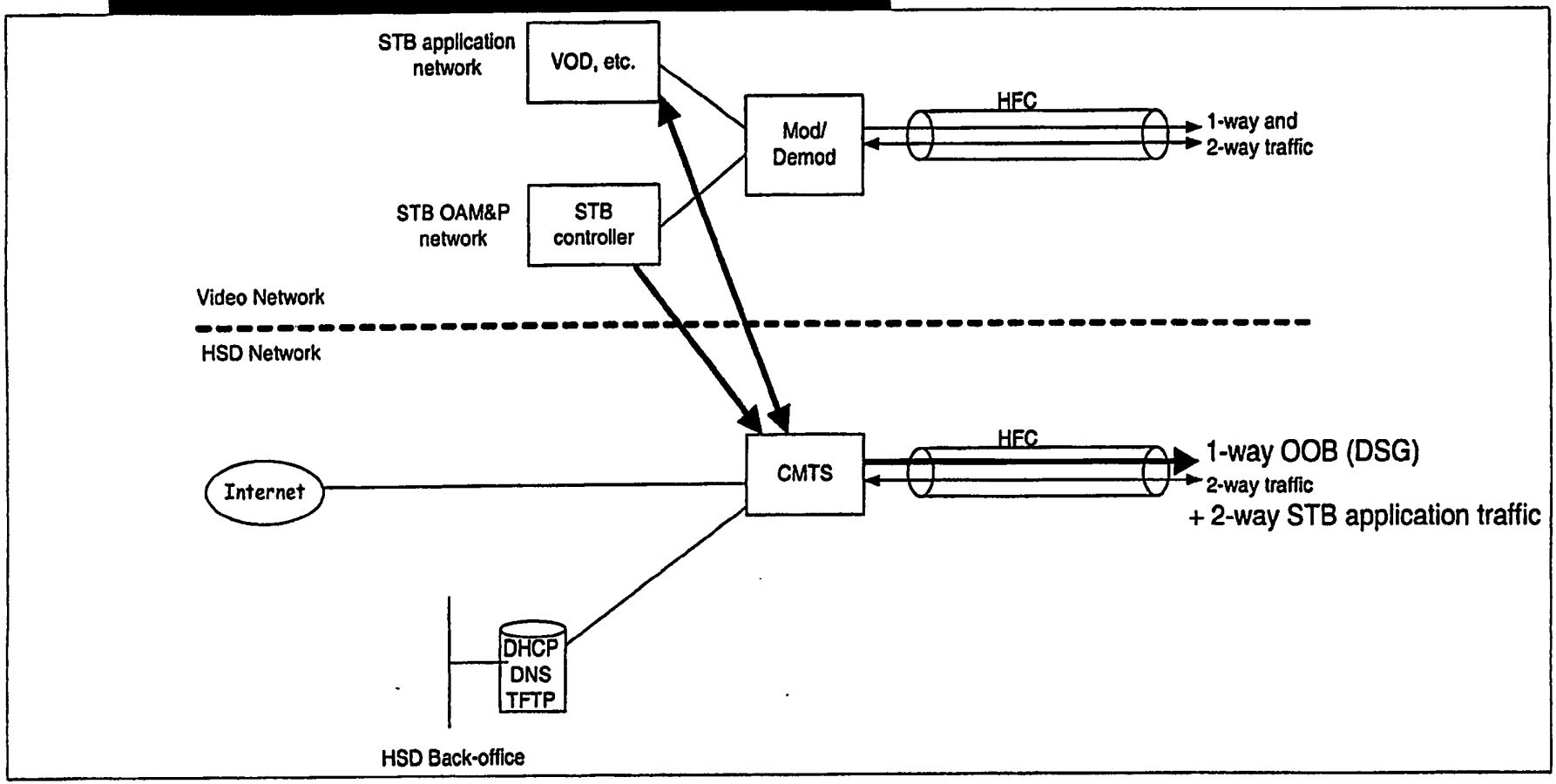
4.10.2 Role of BPI+

BPI+ is used for both eCM device authentication and for privacy for two-way traffic. Since BPI+ does not operate over the DSG tunnels, the supplier must secure OOB messages within the DSG tunnels as needed.

While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. For example, components referred to herein as singular items could alternatively be implemented as multiple items. The words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention.

DSG Architecture

System-Level Overview



- Legacy OOB stays for already deployed STBs

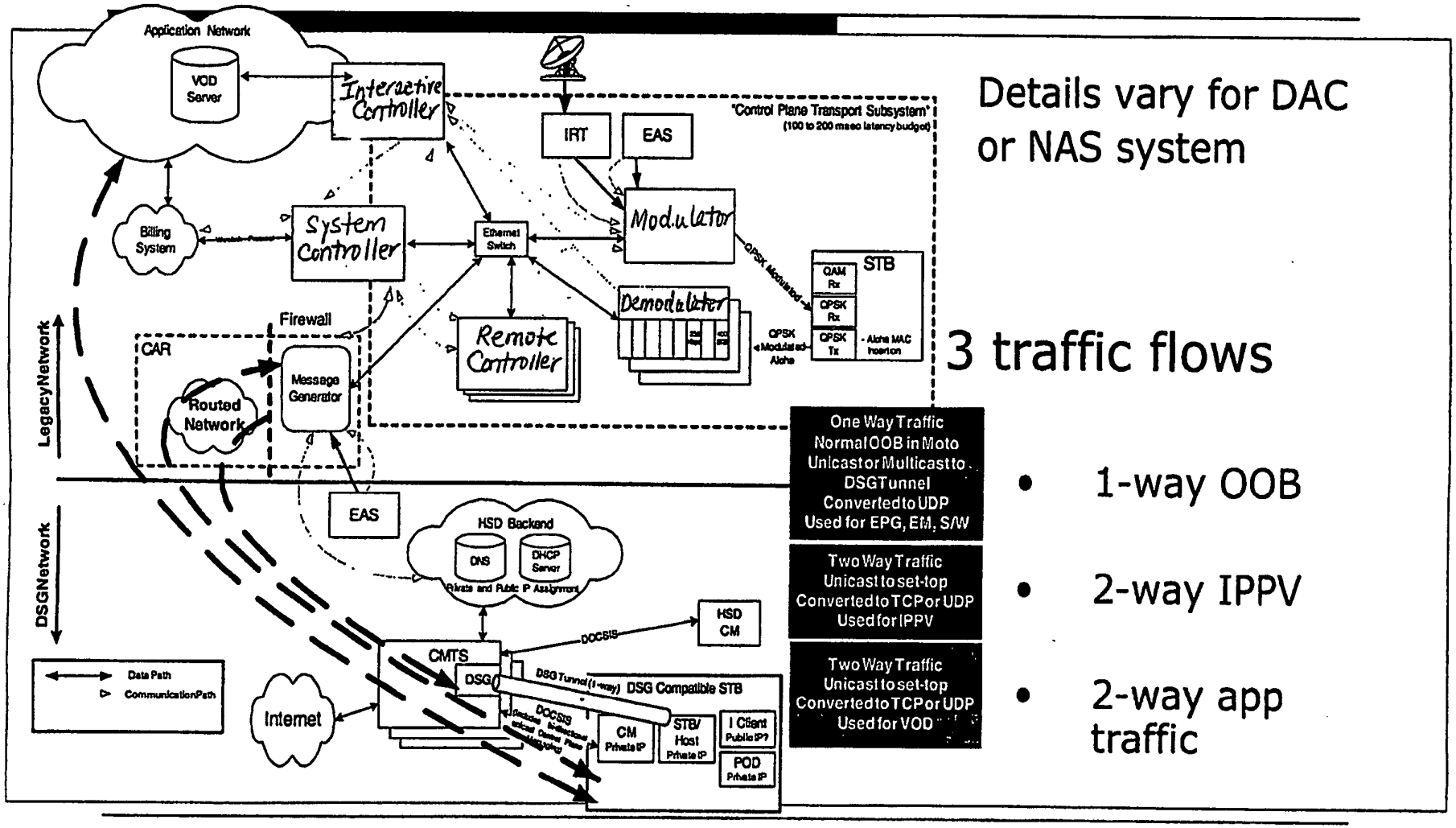
Advantages

- If a STB is to implement DOCSIS, DSG removes the cost of the STB OOB receiver
- Allows continued use of existing STB network controller
- The legacy OOB channel is "narrowband" (<2 Mbps) uses a relatively small percentage of a downstream
  - Completely transparent to other DOCSIS devices
  - The legacy OOB channel can still be carried on the cable plant to support already deployed legacy STBs

Benefits

- If return path goes out, STB still operational
  - There is NO reliance on 2-way DOCSIS
- Concentrate on DOCSIS as method for high-speed 2-way interactive services
- Re-use of DOCSIS network components
  - CMTS, prov system, network management, etc.

Traffic Flows From Legacy Network

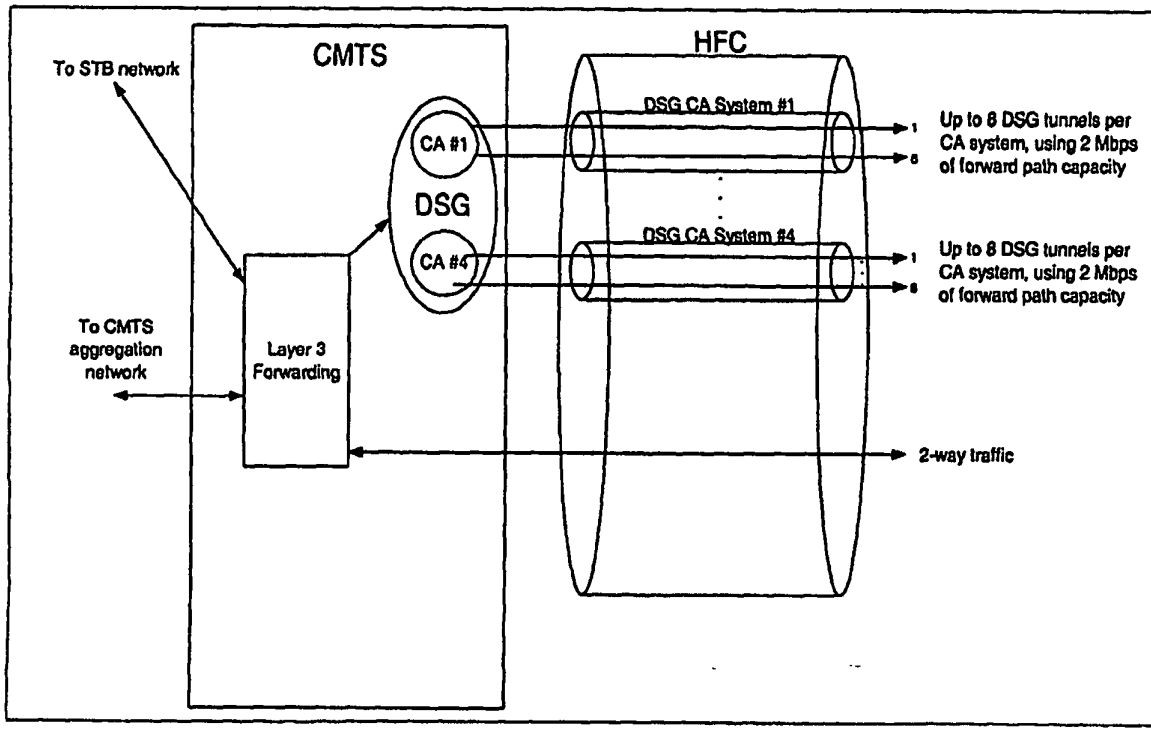


Details vary for DAC or NAS system

3 traffic flows

- 1-way OOB
- 2-way IPPV
- 2-way app traffic

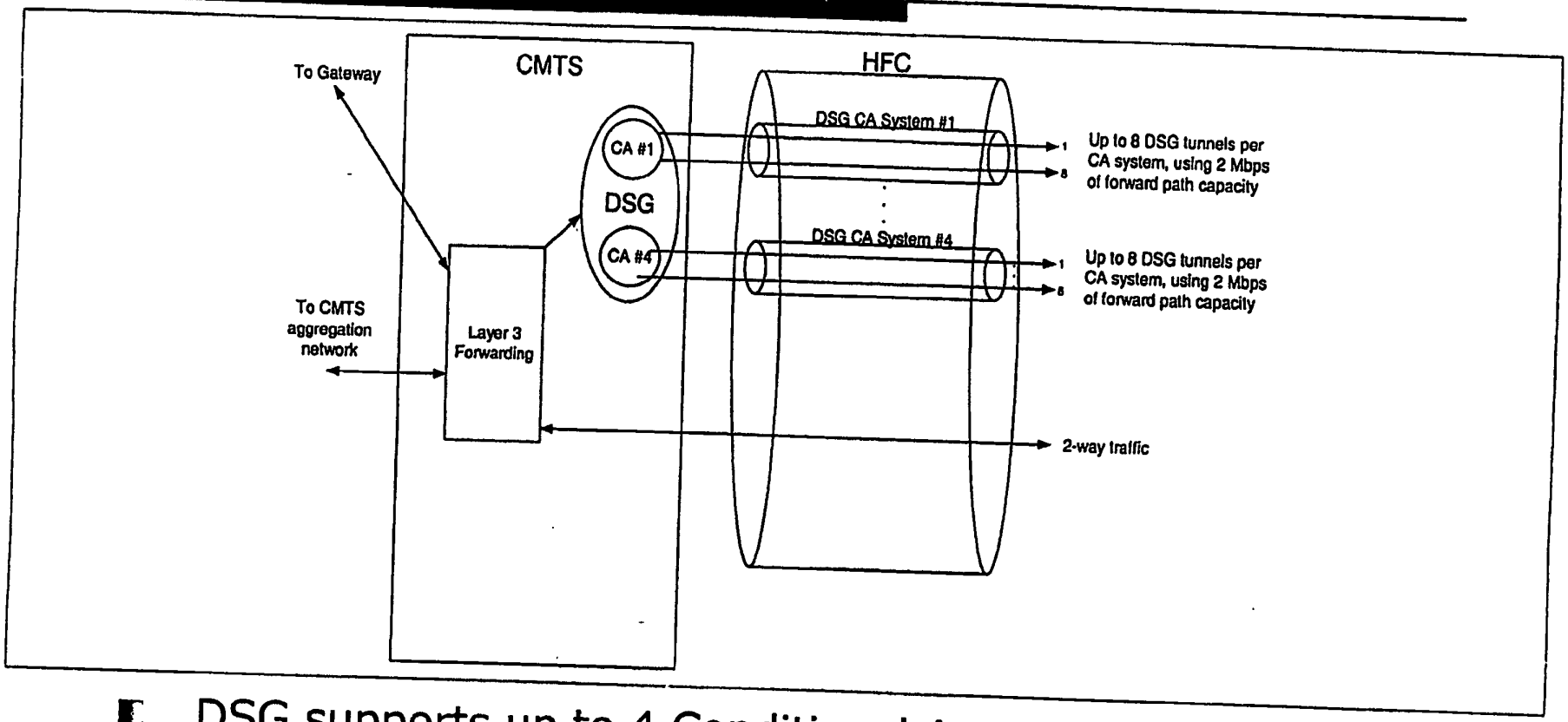
Network



- Method to configure DSG
  - CA system
  - IP address
  - MAC address

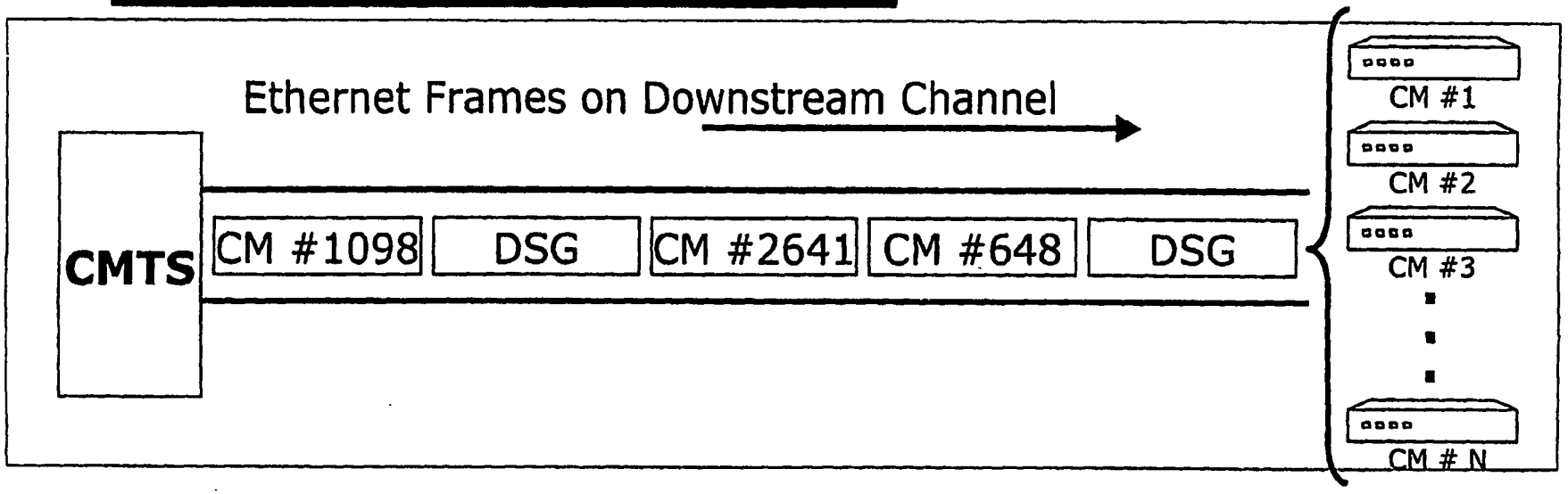
- Mode 1 – Unicast MAC address on HFC
- Mode 2 – Multicast MAC address on HFC (DSG ECR)

DSG - CMTS detail view



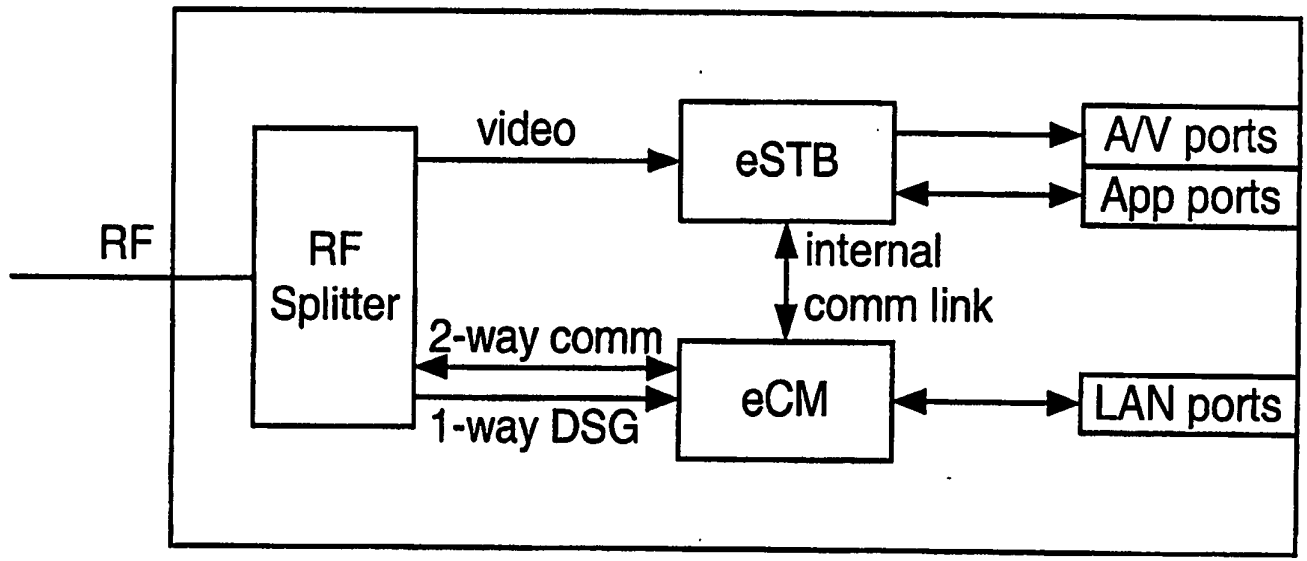
- DSG supports up to 4 Conditional Access Systems
- Each CAS must support up to 8 DSG tunnels

DOCSIS Forward Path Logical View



- All CMs see all Ethernet frames on the downstream
  - just accept what the ones they know about
  - Based on destination MAC address in Ethernet frame
  - CMs that don't know the DSG MAC address will drop DSG frames

DOCSIS-Enabled-STB (DE-STB) Logical View

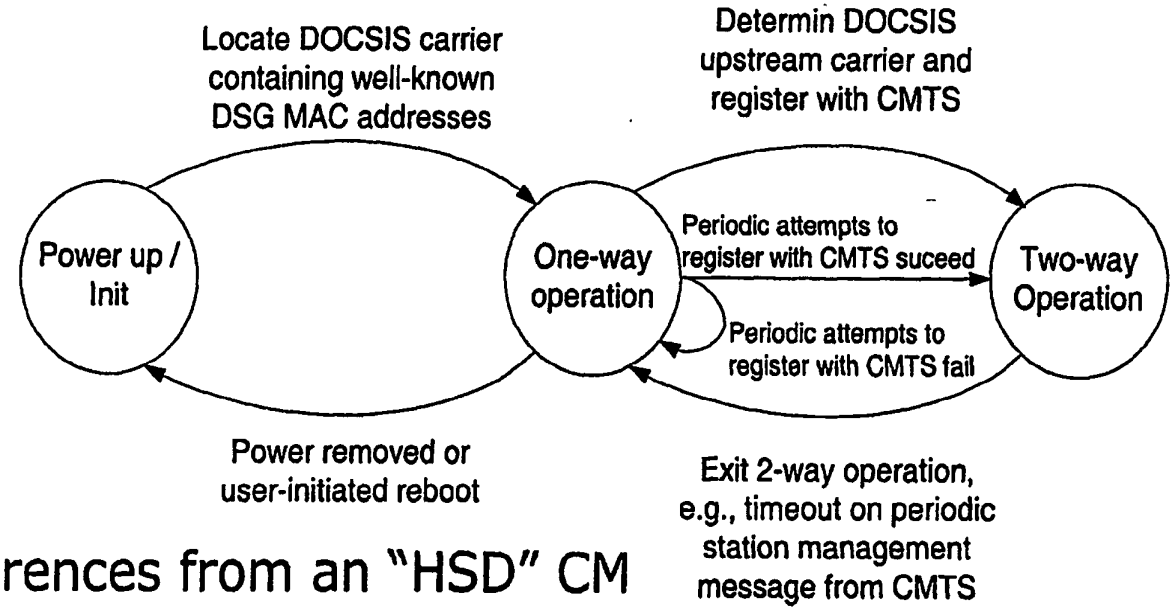


- Looks a lot like an MTA
  - Embedded CM (eCM)
  - Embedded STB (eSTB)

Designing Prov/OSS spec to match what's already done for DOCSIS, CableHome, etc.

OpenCable Host Device Core Functional Requirements

- Chapter 13 says how a DOCSIS CM operates within a STB
  - OpenCable calls this an "Advanced Host"



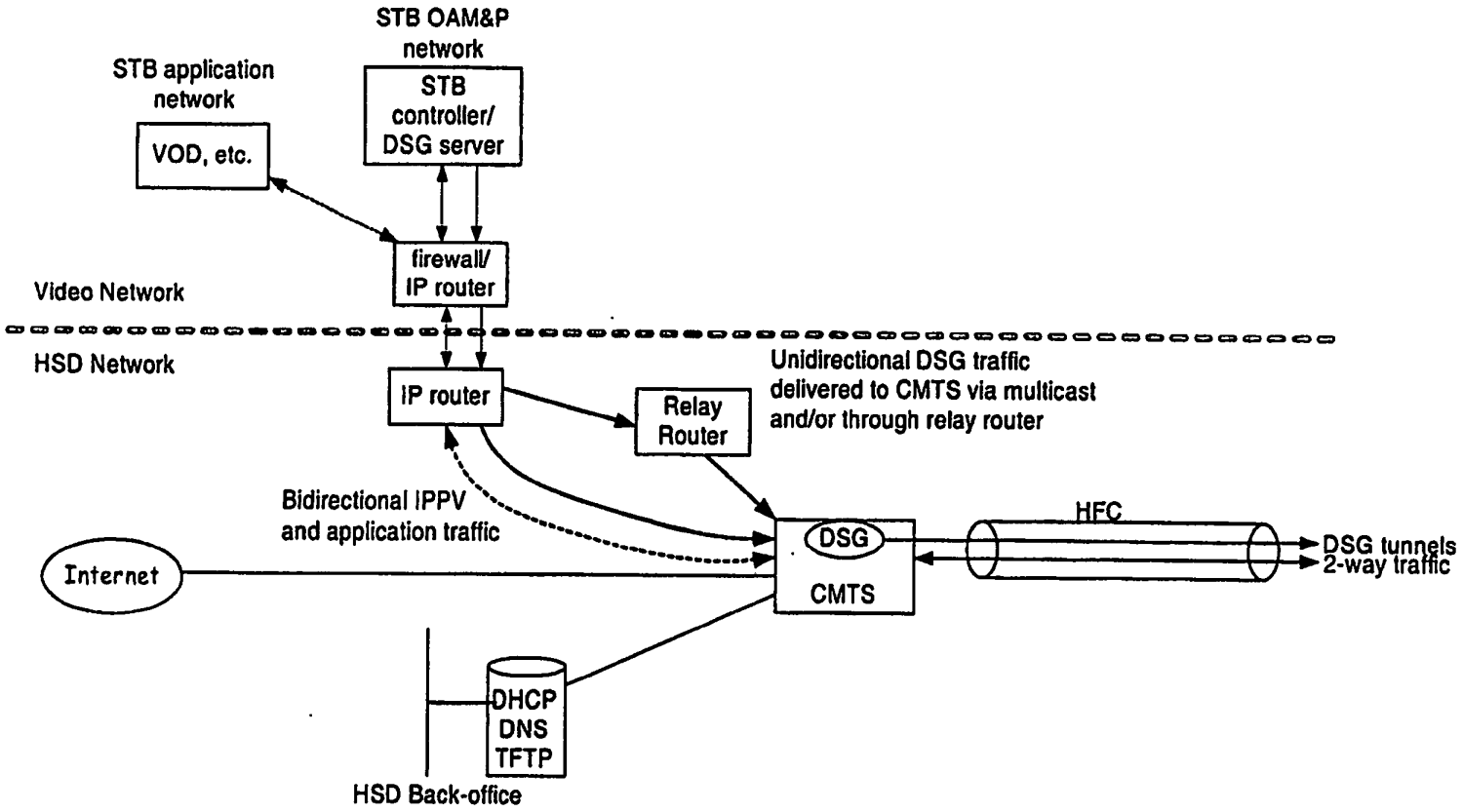
- Differences from an "HSD" CM
  - If return path goes out, CM operates in "1-way mode"
  - CM can still acquire DSG tunnel frames when return path out
  - Timers to handle when DSG tunnel frames stop appearing

Existing Specifications
CableLabs® creates interface spec's

- DOCSIS Set-top Gateway (DSG)
  - STB OOB message transport over DOCSIS
- OpenCable™ Advanced Host Device Core Functional Requirements
  - Set-top box specification with embedded DOCSIS CM
- OpenCable™ Common Download Specification
  - How the OCAP implementation is downloaded

DSG Network

Video Control Plane: DSG, IPPV, VOD signaling



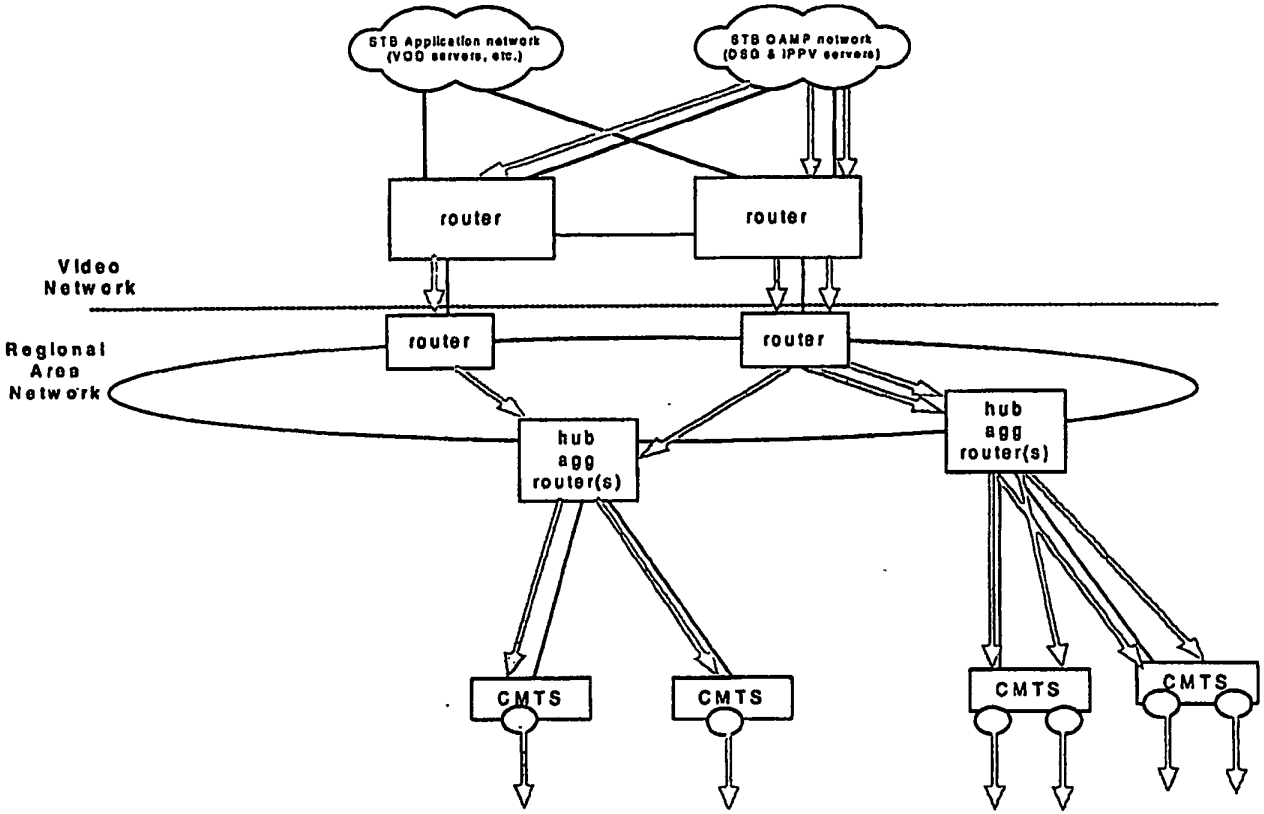
Video Control Plane: DSG

- Problem:
  - Get a stream of IP packets generated by a single source to many destinations
- Requirements:
  - Efficient, scaleable, standards based, operational, secure
- Options:
  - Multicast delivery
  - N x Unicast delivery (relay router)

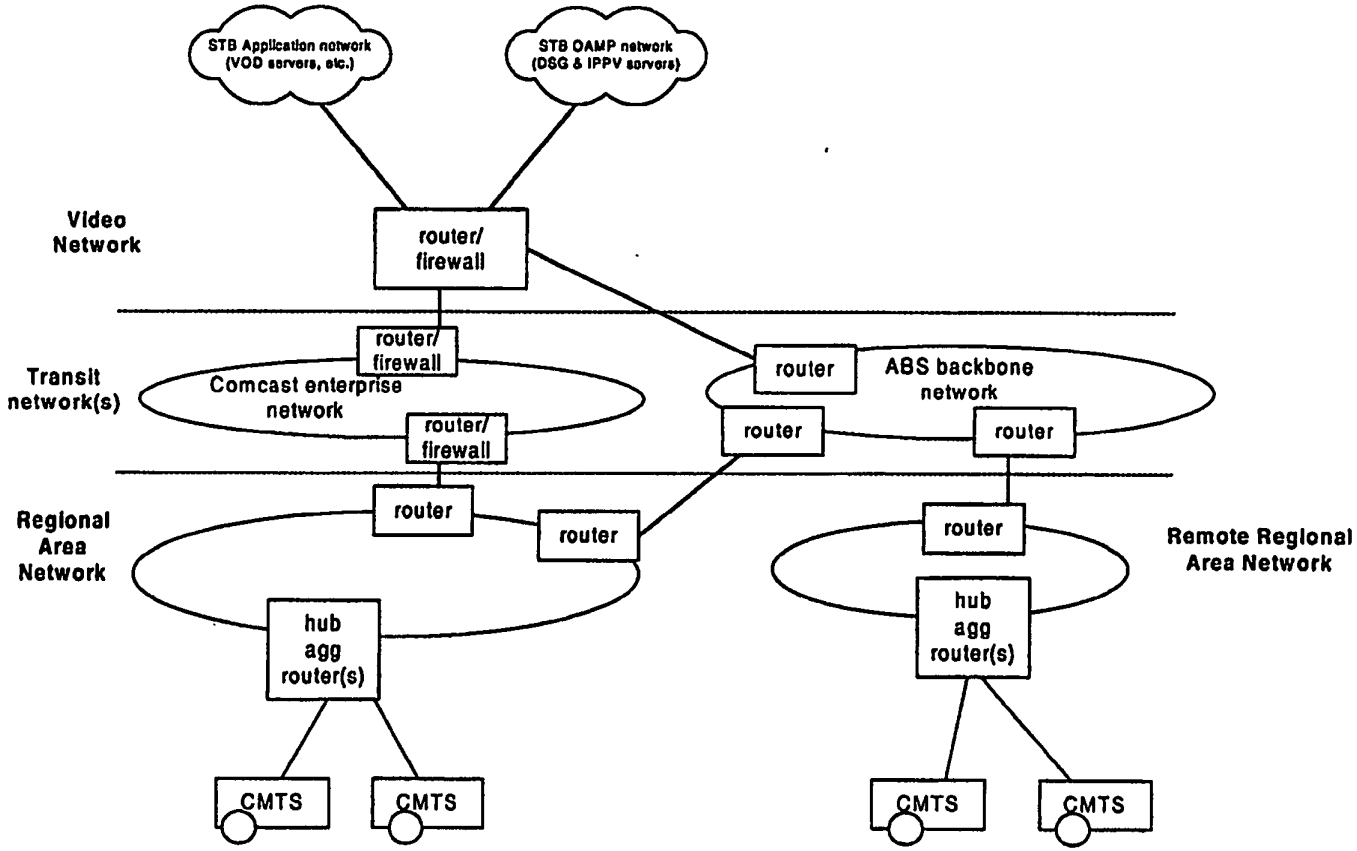
Option1: Source-Specific m-cast (SSM)

- SSM Protocol Details:
  - "one-to-many" instead of "any-to-many"
    - Receivers specifies src of interest; only packets from this src flow over multicast tree
      - Some inherent security
      - Device configs, network ops simpler; more efficient
- Network Configuration details:
  - An SSM "channel" per DSG tunnel
  - CMTS specifies which channels are of interest
  - Multicast trees built from CMTSs back to source
- Standard's based
  - PIMv2
  - IGMPv3

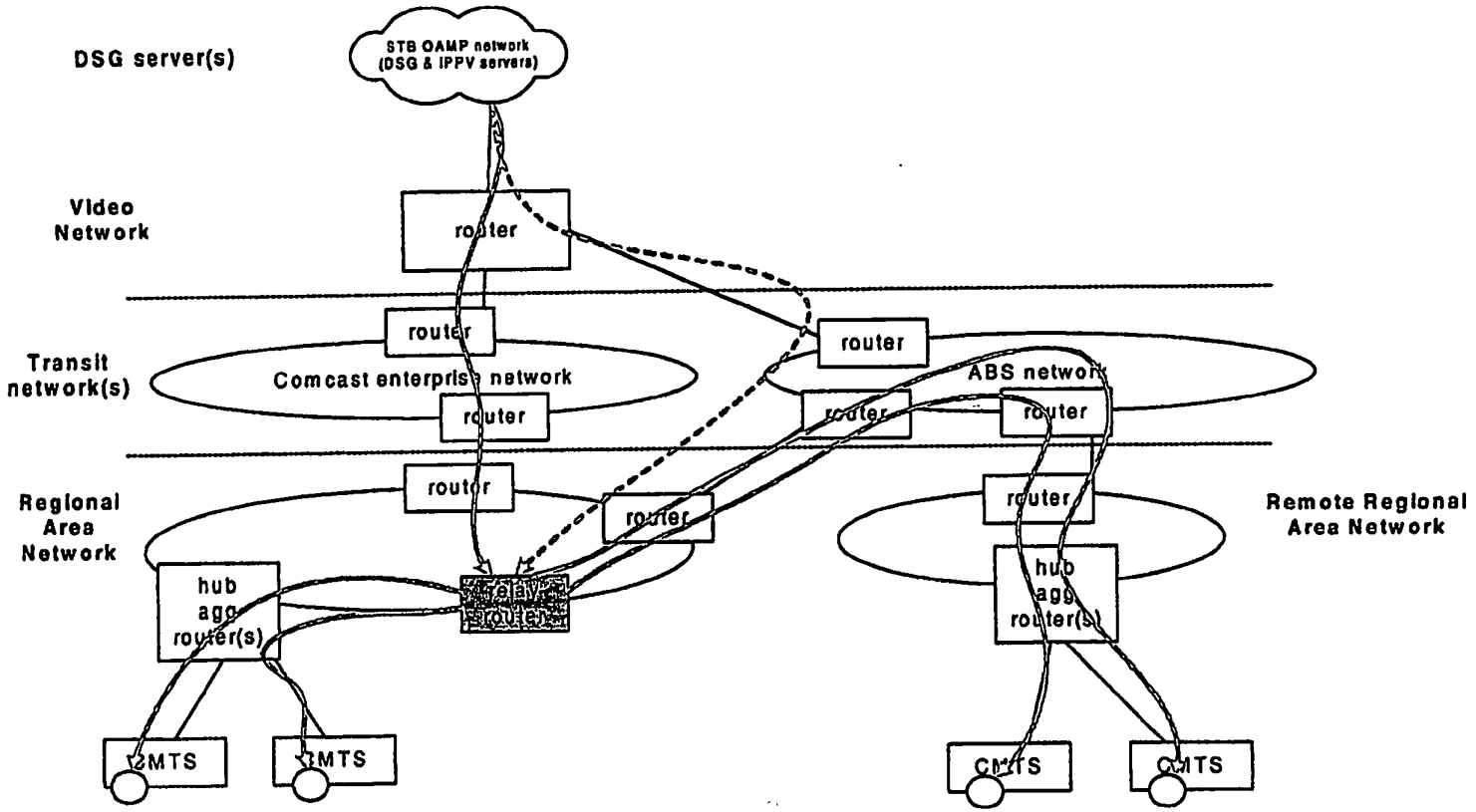
Option 1:
Multicast distribution tree



Option 1: Issues



Option 2: N x Unicast delivery (relay router approach)



DSG Tunnel Rules on CMTS

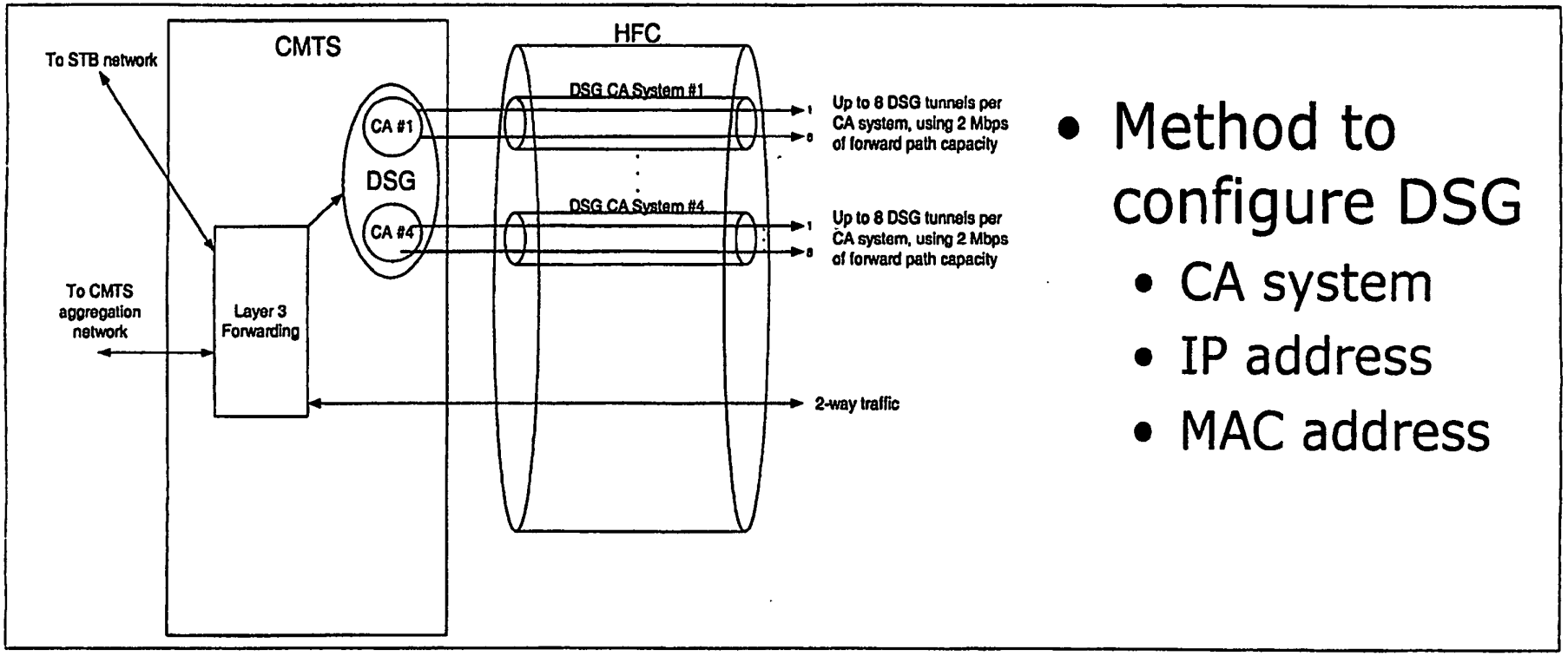
- Defines DSG tunnel mapping
  - DSG input can come from
    - IP unicast
    - IP multicast
  - DSG can apply:
    - per CMTS chassis
    - per CMTS card
    - per downstream
  - DSG can use
    - Unicast MAC address
    - Multicast MAC address

DSG Implementation

- Rate Shaping the DSG tunnel
  - Limit to 2.048 Mbps
  - Describes in detail how this is done
- CMTS should support up to 4 CAS with 8 DSG tunnels each
- Sharing DSG tunnels across different CA systems
  - e.g., shared EPG information, but separate EMMs

DSG - CMTS detail view

ARP table entry



- Method to configure DSG
  - CA system
  - IP address
  - MAC address

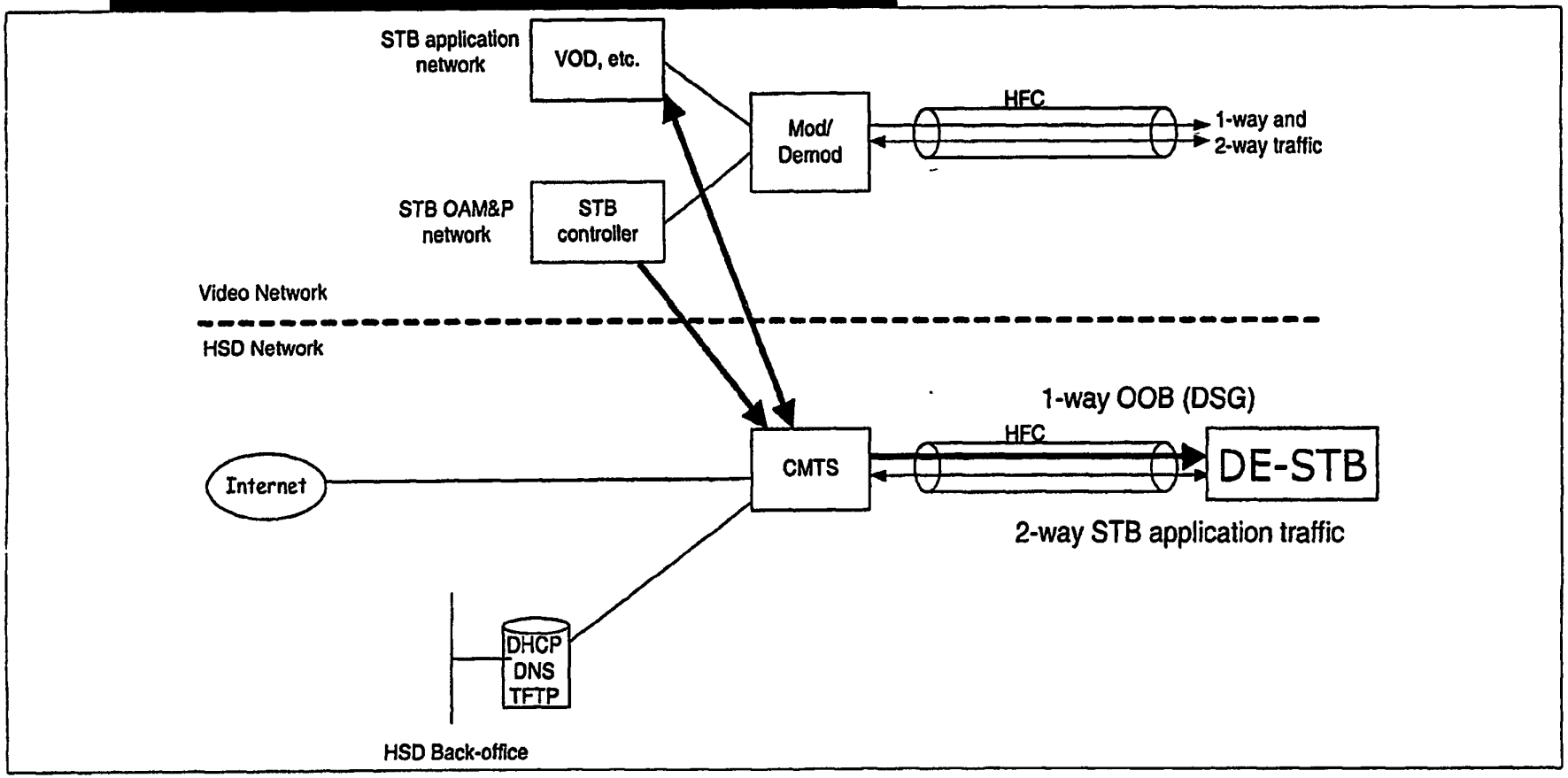
- Mode 1 – Unicast MAC address on HFC
- Mode 2 – Multicast MAC address on HFC (DSG ECR)

DSG Security Considerations

- At DSG in CMTS, keep other traffic from getting into a DSG tunnel
  - Protect against spoofing DSG tunnel MAC addresses
  - Migrate to using Multicast MAC address
- In homes, ensure DSG information is not exposed on a home LAN
  - Application-layer privacy (encrypt the EMMs, etc.)
  - IP filtering in HSD CMs to block DSG

DSG STB Operation

System-Level Overview



Specifications

Align with existing where possible

- DOCSIS Set-top Gateway (DSG)
  - STB OOB message transport over DOCSIS
- OpenCable™ Advanced Host Device Core Functional Requirements
  - specification for embedded DOCSIS CM in a STB
- OpenCable™ Common Download Specification
  - How the OCAP implementation is downloaded

DE-STB Do's

- Use the same STB controller as today
- Replace legacy QPSK transport with standard's based transport
- Migrate provisioning model

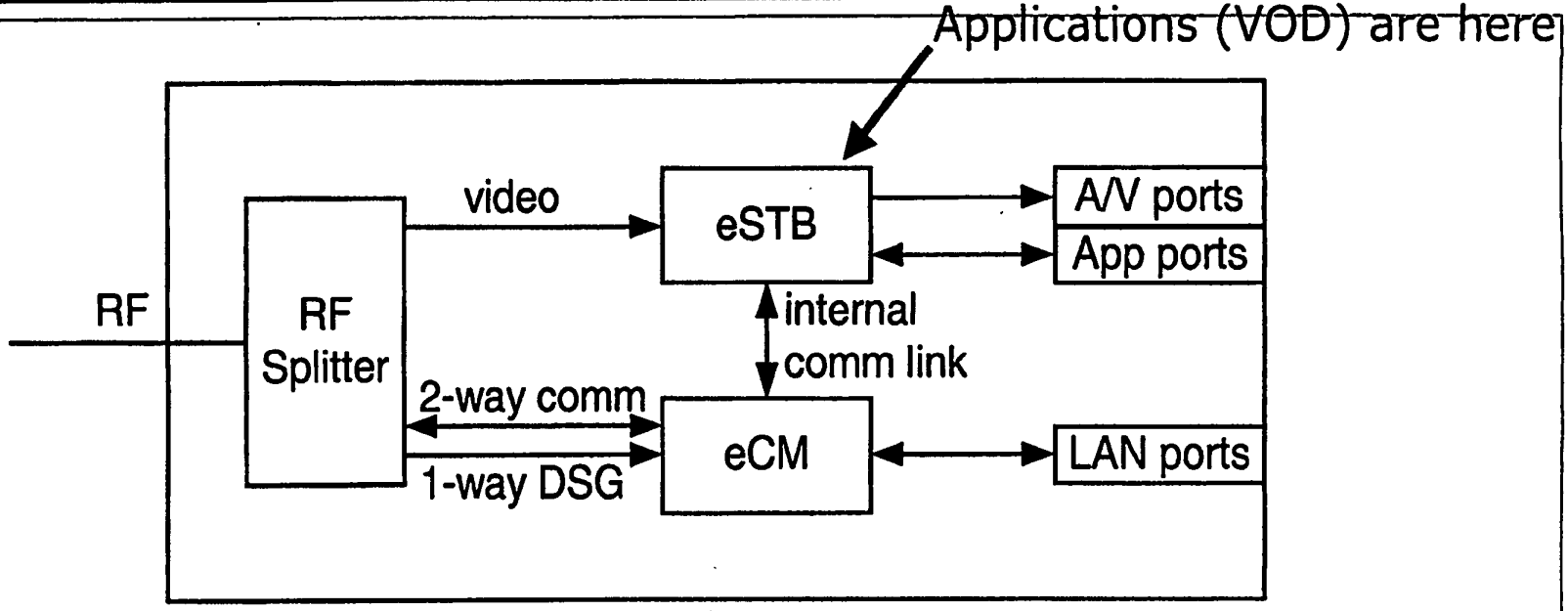
  DHCP, ToD, TFTP, SNMP, etc.

DE-STB Foundation

- Logical Entities
  - eCM
  - eSTB
- State machine
  - Interacting with 1-way and 2-way plant

DOCSIS-Enabled-STB (DE-STB)

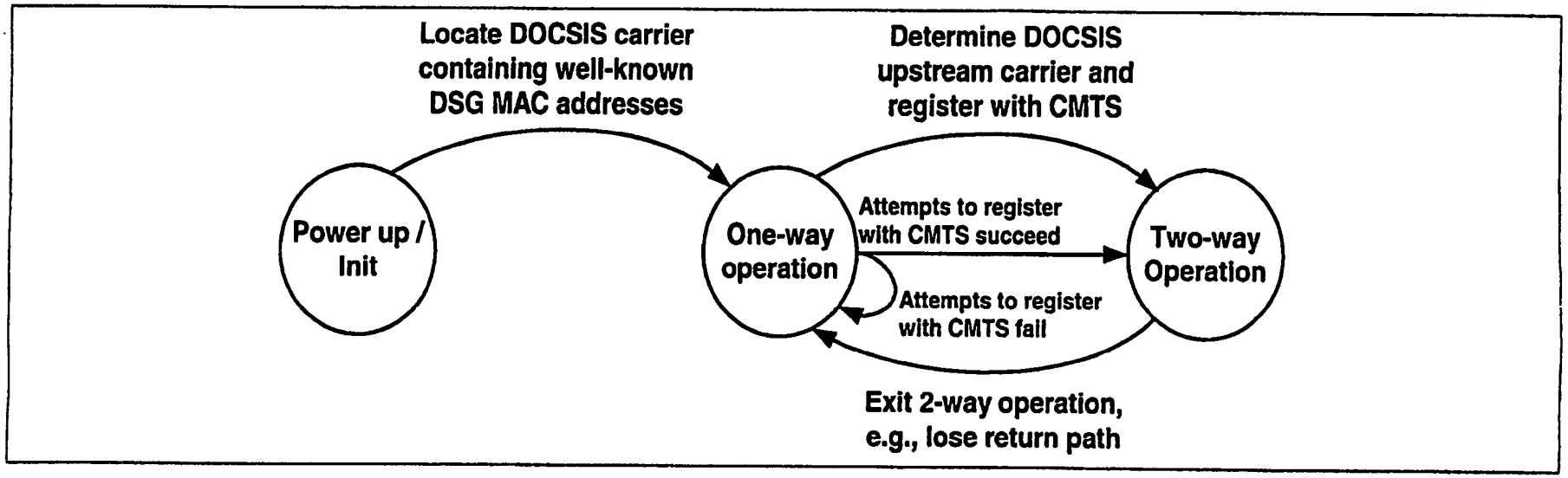
Logical View



- Looks a lot like an MTA or PS
  - Embedded CM (eCM)
    Embedded STB (eSTB)

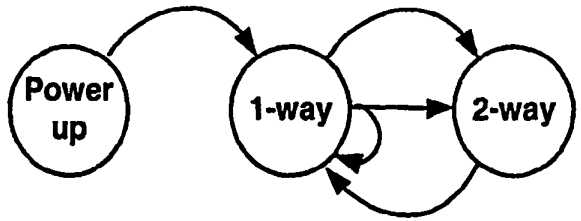
Unique interactions due to nature of STB operations

Core DE-STB State Machine



- Differences from an "HSD" CM
  - If return path goes out, CM operates in "1-way mode"
  - CM can still acquire DSG tunnel frames when return path out
  - Timers to handle when DSG tunnel frames stop appearing
- Aligns with OpenCable™ Host Core Functional Requirements

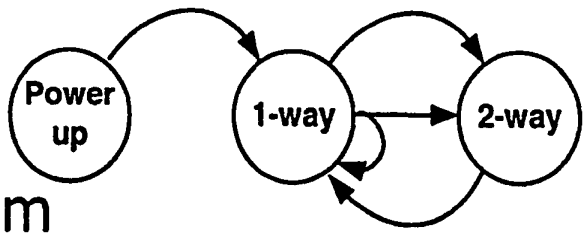
DE-STB Boot Steps



- What the eCM and eSTB do to boot
  - Based on experience with existing STBs
  - Based on experience with embedded DOCSIS devices
- STBs implementing DOCSIS can follow common provisioning
  - remove ambiguity for suppliers
  - solve back-office issues and agree on way to move forward
  - supports product selection from multiple suppliers
- Preserve customer expectations of STB operation

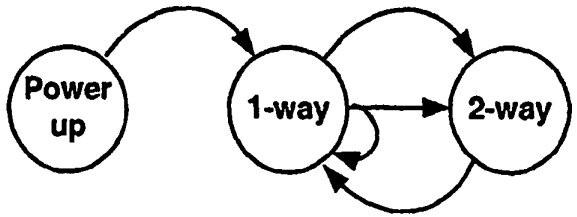
DE-STB Boot Step #1

eCM finds correct DOCSIS downstream



- eSTB "knows" the DSG tunnel addresses
  - From operating software image (embedded security)
  - From CableCARD™
  - Learns from CMTS (future capability to be designed)
- eSTB tells eCM the DSG tunnel addresses
- eCM scans downstreams for one containing a DTD that lists all the DSG tunnel addresses it needs

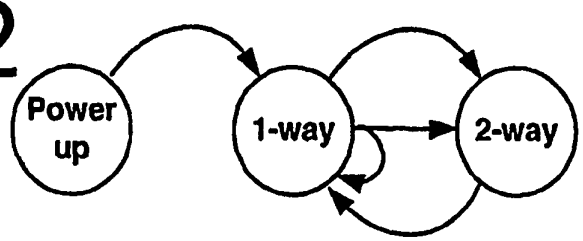
DTD Usage



- eCM does not look for the DSG tunnels on the downstream; rather, it looks for a DTD containing those MAC addresses
  - eCM has not booted yet, just scanning downstreams
- If network issue stops OOB packets from legacy network from reaching the CMTS, the CMTS continues sending DTDs and eCM stays on that downstream channel
- DTD also a 1 packet-per-second heartbeat

DE-STB Boot Step #2

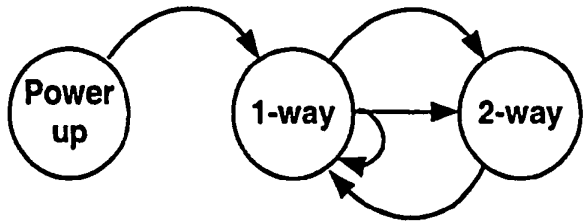
eCM forwards DSG info to eSTB, enters 1-way mode



- Once a DTD is found, the eCM accepts data from the DSG tunnel(s) and forwards to eSTB
- eSTB configures and becomes 1-way operational
  - No reliance on return path
- If DTD but no DSG tunnels (network problem), eCM stays on that downstream and eSTB becomes operational on previous configuration

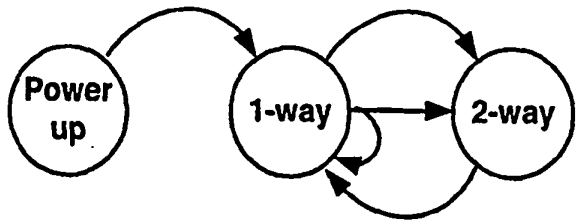
DE-STB Boot Step #3

eCM attempts to register on CMTS



- eCM follows normal DOCSIS registration
  - All the while forwarding DSG info to the eSTB
- If successful, eCM signals to eSTB that it can attempt to initialize
  - eSTB gets config info from eCM config file
- If unsuccessful, eCM starts a timer and retries
  - Stays on that downstream as long as receiving DTD listing the DSG tunnel addresses
  - eSTB stays in 1-way operation

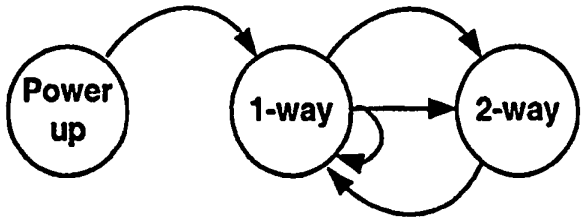
DE-STB Boot Step #4



eSTB configures itself and 2-way services

- eSTB uses DHCP to get IP address and other configuration parameters
- eSTB uses info from eCM config file
  - E.g., SNMP access control
- Once eSTB comes up, 2-way applications initialize
- If unsuccessful, STB goes back to 1-way operation and retries

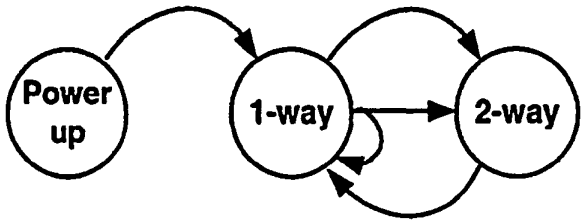
DE-STB Boot Step #5



return path goes out,
or was never available

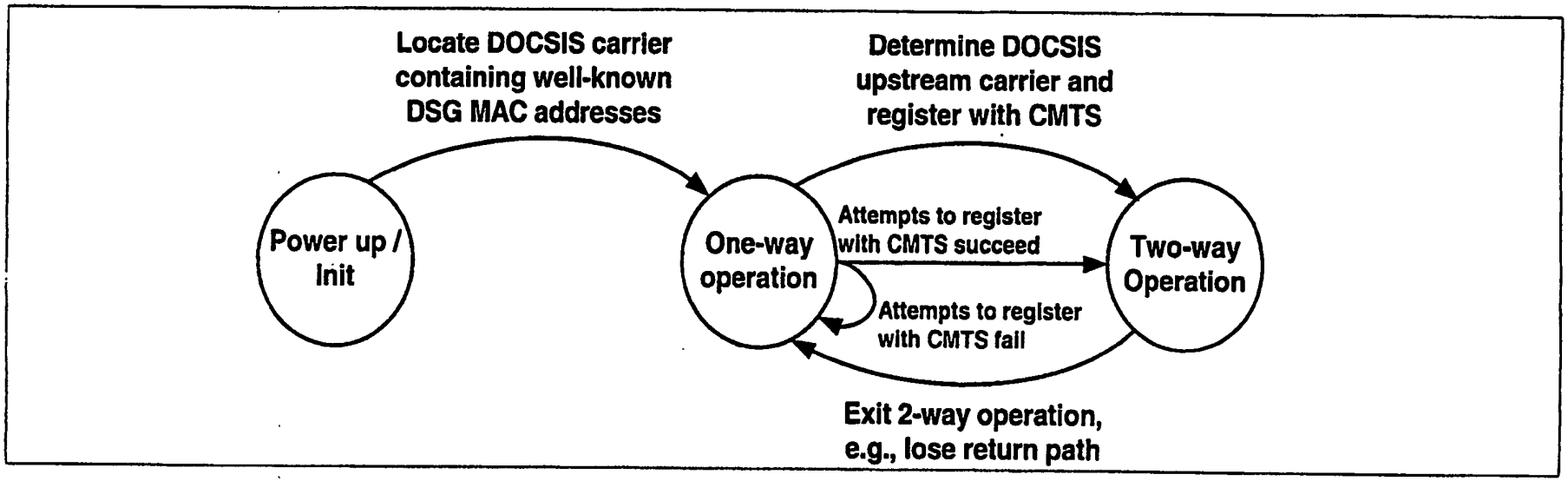
- eCM stays on downstream channel, forwarding DSG tunnel information to eSTB
  - Gets DTD once per second listing DSG tunnel addresses
- eCM sets a timer and periodically attempts to register with CMTS

DE-STB Boot Step #6 DTD message change



- If DTD message either:
  - Stops appearing
  - No longer lists all the needed DSG tunnel addresses
- eCM will scan for new downstream
  - eSTB in 1-way operation on previous configuration

eCM STB Timers



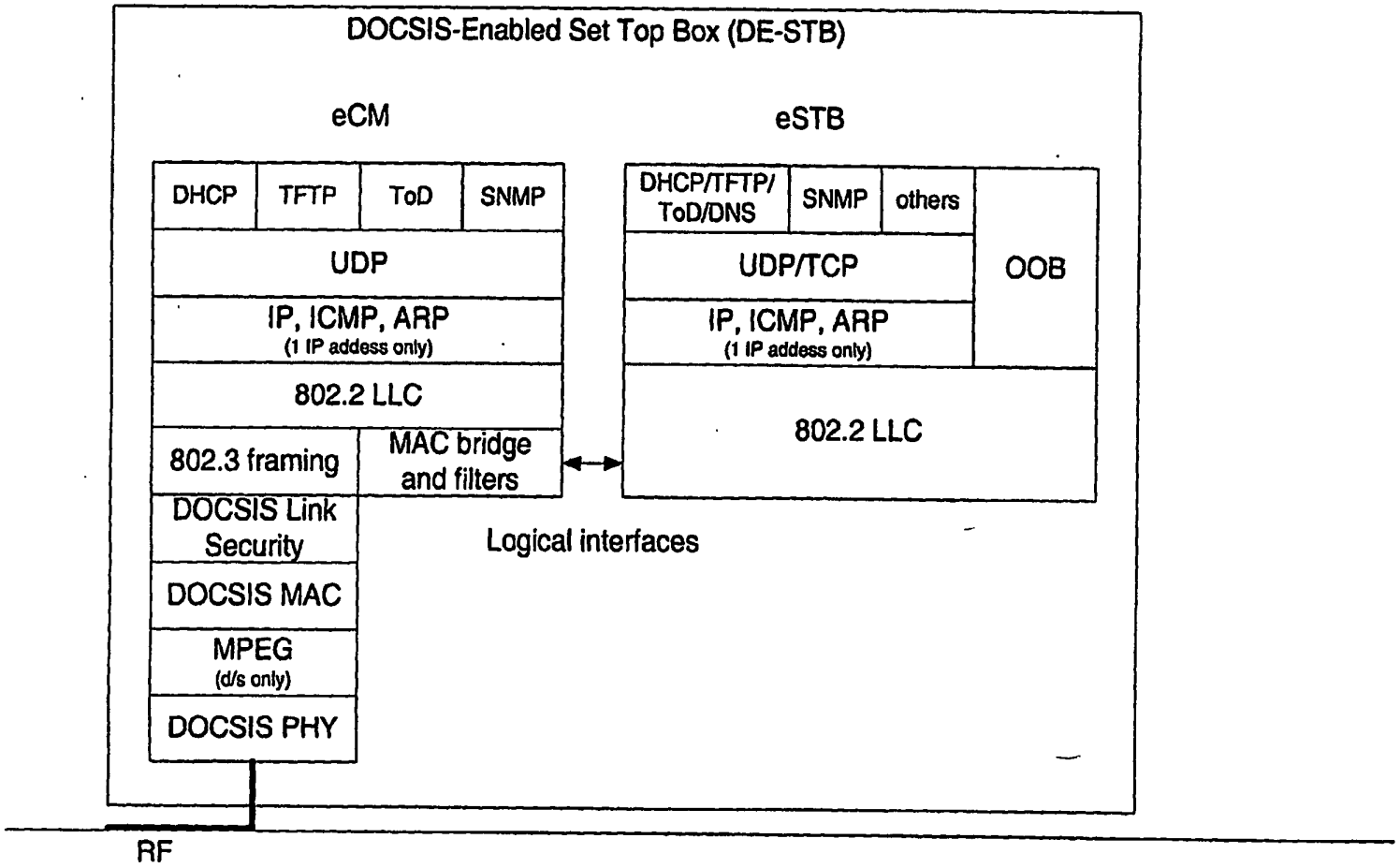
- Tdsg3 – Two-way retry timer
- Tdsg4 – One-way retry timer
- Tdsg5 – DTD message interval

Summary

- Aligns w/ OpenCable™ Host Core Rqmts
- CM operation unique to STB
  - Meets conditions of one-way plant

DSG Provisioning & Operations Support Systems

DE-STB Protocol Stack & Interfaces



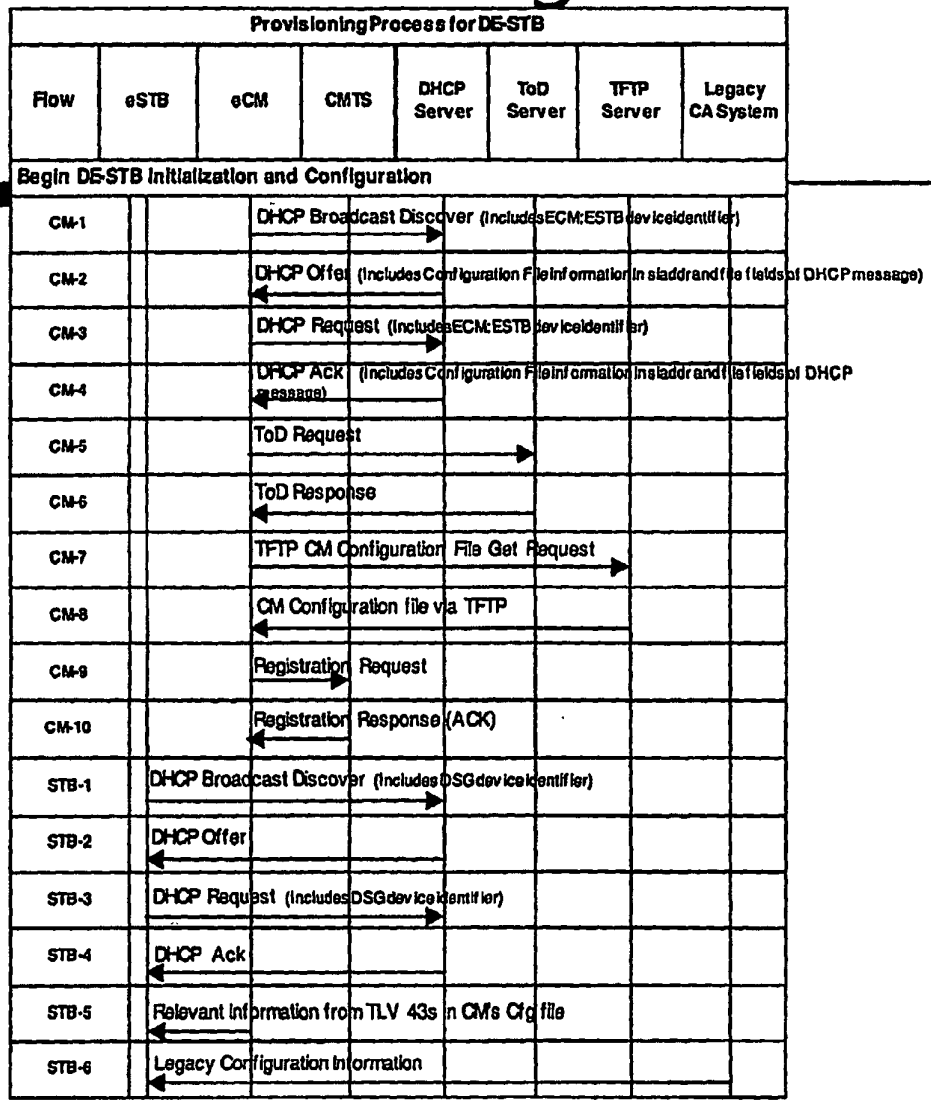
Prov-OSS Specification Content

- Provisioning Considerations
  - Top-down vs. Bottom-up
    - Top-down, pre-provisioned
  - Provisioning variations for STBs
    - Embedded security (no CableCARD)
    - Monolithic DE-STB device code image
  - DHCP Considerations
    - Updates to existing CM DHCP options
  - ToD Considerations
  - Config File & TFTP Considerations
    - Single config file
  - Domain Name System Considerations

Prov-OSS Specification Content (cont.)

- Provisioning Requirements – specific requirements for the eCM & eSTB entities
  - Provisioning Interface Requirements
    - DHCP Requirements – Option 43 & 60 details
    - DNS Requirements – Use of DHCP option to propagate hostname information based on the eSTB's unit address
  - Provisioning Process Requirements
    - Process flow for the DE-STB
  - Configuration File Requirements
    - Monolithic (CM and STB) configuration files
      - Containing TLV 43s destined for the eSTB entity
      - Used to set standard MIB objects in the eSTB, such as SNMP nmAccess

DE-STB Provisioning Process Flow



Prov-OSS Specification Content (cont.)

- Operation Support Systems Considerations – Overall management concepts
  - SNMP
    - Separate (CM and STB) SNMP agents in the DE-STB
- Configuration management
  - Software Download
    - Monolithic firmware image – download via legacy methods
  - Fault Management
    - eSTB Event Notification – handled by the eCM

Prov-OSS Specification Content (cont.)

- Operation Support Systems Requirements – Describe specific SNMP & MIB requirements
  - SNMP Protocol
    - SNMP for eCM – Per DOCSIS OSSI Spec
    - SNMP for eSTB – Similar to DOCSIS OSSI (but only v1 & v2c mandated)
  - Management Information Bases (MIBs)
    - MIBs for eCM – Per DOCSIS OSSI Spec
    - MIBs for eSTB – Similar to DOCSIS OSSI
  - Configuration management
    - Definition of eSTB sysDescr object
  - Fault Management
    - Event Notification – 2 new eSTB Prov state events in the eCM
    - eSTB support for Pings

Prov-OSS Spec Issues

- Type of eSTB Diagnostic capability needed from the CMCI side of the DE-STB
  - On-screen Display
  - eSTB MIB that includes the same info and more
- How to prevent spoofing of the DSG system by malicious users
  - DHCP controls – device identification
  - IP and/or LLC layer CM filters
    - Impact on all existing deployed CMs
- The DSG network's use of Domain Name System (DNS)
  - A & PTR Records will be created for each eSTB - which network components will make use of DNS to communicate with the eSTBs

Prov-OSS Spec

- Firmware image download methods supported
  - Data Carousel
  - DOCSIS Secure Software Download
  - Multicast Software Download
- Could support separate eCM & eSTB firmware images and deviate from the Phase 1 monolithic requirement
- Complete eSTB MIB
  - What parameters need to be monitored/configured
  - Most parameters could be read-only (for security reasons)
- Support for CableCARD/POD
  - CableCARD could make use of a separate IP address